Nessus 5.0 Flash Benutzerhandbuch

4. Dezember 2012

(Revision 18)

Inhaltsverzeichnis

Einleitung 3
Regeln und Konventionen 3
Die Nessus-Benutzeroberfläche im Überblick 3
Beschreibung 3
Unterstützte Plattformen 4
Installation 4
Bedienung 4
Übersicht 4
Verbindung mit der Nessus-Benutzeroberfläche herstellen 4
Überblick zu den Richtlinien 9
Standardrichtlinien 9
Neue Richtlinie erstellen 11
Allgemein 11
Credentials 15
Plugins 18
Preferences 22
Richtlinien importieren, exportieren und kopieren 25
Scans erstellen, starten und planen 26
Berichte 29
Browse (Durchsuchen) 29
Berichtsfilter 35
Compare (Vergleichen) 42
Upload und Download 43
Das .nessus-Dateiformat 44
Delete (Löschen) 45
Mobil 45
SecurityCenter 45
SecurityCenter 4.0 bis 4.2 für die Kooperation mit Nessus konfigurieren 45
SecurityCenter 4.4 für die Kooperation mit Nessus konfigurieren 46
Hostbasierte Firewalls 47
Details zu Scaneinstellungen 48
Weitere Informationen 73
Wissenswertes zu Tenable Network Security 74

Einleitung

Das vorliegende Dokument beschreibt die Verwendung der **Nessus-Benutzeroberfläche (UI)** von Tenable Network Security. Anmerkungen und Vorschläge richten Sie via E-Mail an support@tenable.com.

Die Nessus-Benutzeroberfläche ist eine webbasierte Oberfläche für den Nessus-Sicherheitslückenscanner. Zur Verwendung des Clients muss ein betriebsbereiter Nessus-Scanner in Ihrer Umgebung vorhanden sein, und Sie müssen mit der Bedienung des Scanners vertraut sein.

Regeln und Konventionen

Das vorliegende Dokument wurde aus einer ursprünglich auf Englisch verfassten Version übersetzt. Teilweise wurden Texte auf Englisch beibehalten, wenn diese in englischer Form im Produkt erscheinen.

In der gesamten Dokumentation werden Dateinamen, Daemons und ausführbare Dateien in einer Schriftart wie **`courier bold`** angezeigt (z. B.: **`gunzip`**, **`httpd`** oder **`/etc/passwd`**).

Befehlszeilenoptionen und Schlüsselwörter werden ebenfalls in der Schriftart **`courier bold`** angezeigt. Die Befehlszeilen sind teils mit, teils ohne Befehlszeilen-Prompt und dem Ausgabetext des betreffenden Befehls aufgeführt. In den Befehlszeilen erscheint der ausgeführte Befehl in der Schriftart **`courier bold`**, um zu verdeutlichen, was der Benutzer eingegeben hat. Die vom System generierte Beispielausgabe ist hingegen in der Schriftart `courier` (ohne Fettdruck) aufgeführt. Es folgt ein Beispiel für die Ausführung des UNIX-Befehls **`pwd`**:

```
# pwd
/opt/nessus/
#
```

Wichtige Hinweise und Aspekte werden durch dieses Symbol und graue Textfelder hervorgehoben.

Tipps, Beispiele und Best Practices (Empfehlungen) werden durch dieses Symbol und weißen Text auf blauem Grund hervorgehoben.

Die Nessus-Benutzeroberfläche im Überblick

Beschreibung

Die Nessus-Benutzeroberfläche (User Interface, UI) ist eine webbasierte Oberfläche für den Nessus-Scanner. Sie umfasst einen einfachen HTTP-Server und -Webclient und erfordert abgesehen vom Nessus-Server keine weitere Softwareinstallation. Seit Nessus 4 weisen alle Plattformen dieselbe Codebasis auf. Hierdurch werden nicht nur die meisten plattformspezifischen Bugs und Fehler beseitigt, sondern es wird auch eine schnellere Bereitstellung neuer Funktionen ermöglicht. Die wesentlichen Merkmale sind:

- Generierung von **`.nessus`**-Dateien, die von Tenable-Produkten standardmäßig als Grundlage für Informationen zu Sicherheitslücken und Scanrichtlinien verwendet werden
- In einer einzigen **`.nessus`**-Datei lassen sich eine Richtliniensitzung, eine Liste mit Zielen und die Ergebnisse mehrerer Scans speichern und problemlos exportieren. Weitere Informationen entnehmen Sie dem Leitfaden zu den Nessus-Dateiformaten.
- Die Benutzeroberfläche zeigt Scanergebnisse in Echtzeit an. Sie müssen also nicht warten, bis ein Scan abgeschlossen ist, um die Resultate aufzurufen.

- Unabhängig von der Basisplattform wird eine einheitliche Oberfläche für den Nessus-Scanner bereitgestellt. Unter Mac OS X, Windows und Linux ist jeweils derselbe Leistungsumfang vorhanden.
- Die Ausführung von Scans auf dem Server wird nicht unterbrochen, wenn Ihre Verbindung aus irgendeinem Grund getrennt wird.
- Nessus-Scanberichte können über die Nessus-Benutzeroberfläche hochgeladen und mit anderen Berichten verglichen werden.

Unterstützte Plattformen

Da die Nessus-Benutzeroberfläche ein webbasierter Client ist, kann sie auf jeder Plattform ausgeführt werden, die einen Webbrowser bereitstellt.

Die webbasierte Nessus-Benutzeroberfläche bietet maximale Leistung bei Verwendung von Microsoft Internet Explorer 9, Mozilla Firefox 9.x, Google Chrome 16.x oder Apple Safari 5.x.

Installation

Die Benutzerverwaltung des Nessus 5-Servers erfolgt über eine Weboberfläche oder SecurityCenter. Der vormals benötigte NessusClient wird hierzu nicht mehr eingesetzt. Der Scanner kann zwar weiterhin über den NessusClient bedient werden, es wird aber für den Client keine Updates und keinen Support mehr geben.

Weitere Informationen zur Installation von Nessus finden Sie im Nessus 5.0-Installations- und Konfigurationshandbuch. Ab Nessus 5.0 ist Oracle Java (vormals Sun Microsystems Java) für die Generierung von PDF-Berichten erforderlich.

Bedienung

Übersicht

Nessus stellt eine einfache, aber leistungsfähige Oberfläche zur Verwaltung der Scanaktivitäten bereit.

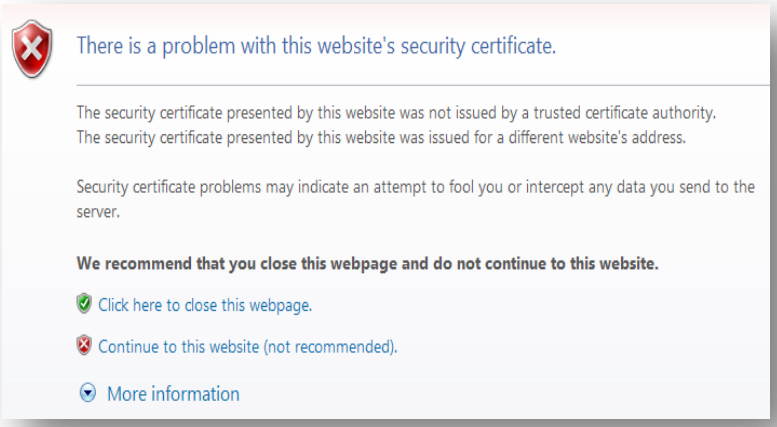
Verbindung mit der Nessus-Benutzeroberfläche herstellen

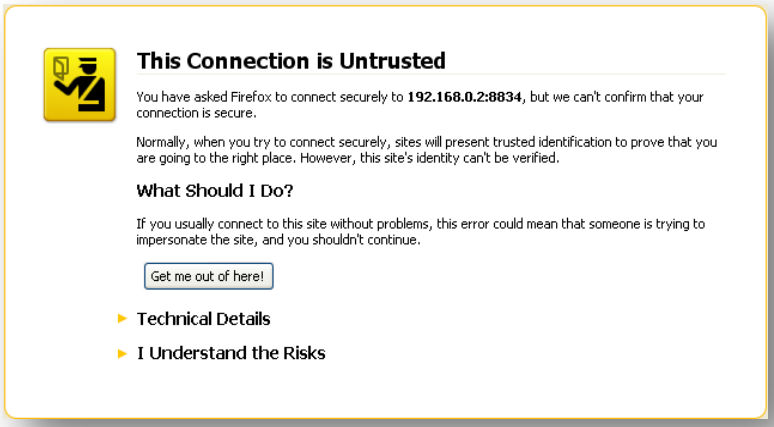
Führen Sie die folgenden Schritte aus, um die Nessus-Benutzeroberfläche zu starten:

- Öffnen Sie einen beliebigen Webbrowser.
- Geben Sie `https://[Server-IP-Adresse]:8834/flash.html` in die Navigationsleiste ein.

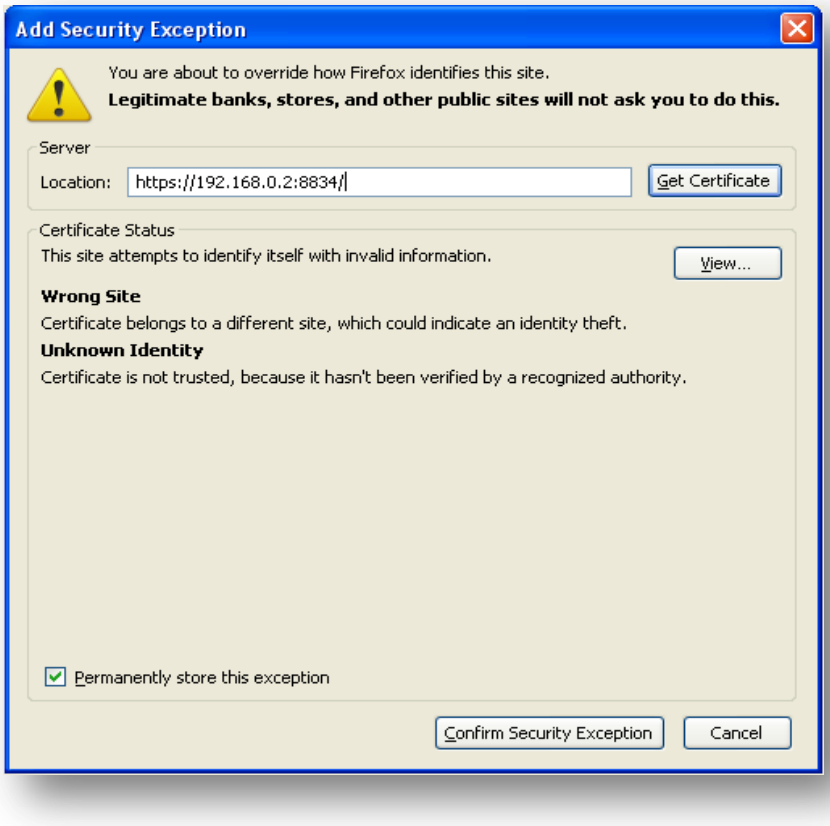
Achten Sie in jedem Fall darauf, die Verbindung mit der Benutzeroberfläche über HTTPS herzustellen, da nicht verschlüsselte HTTP-Verbindungen nicht unterstützt werden.

Wenn Sie zum ersten Mal eine Verbindung mit der Nessus-Benutzeroberfläche herstellen, zeigen die meisten Webbrowser eine Fehlermeldung an, laut der die Website nicht vertrauenswürdig ist, weil das SSL-Zertifikat selbstsigniert ist:


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

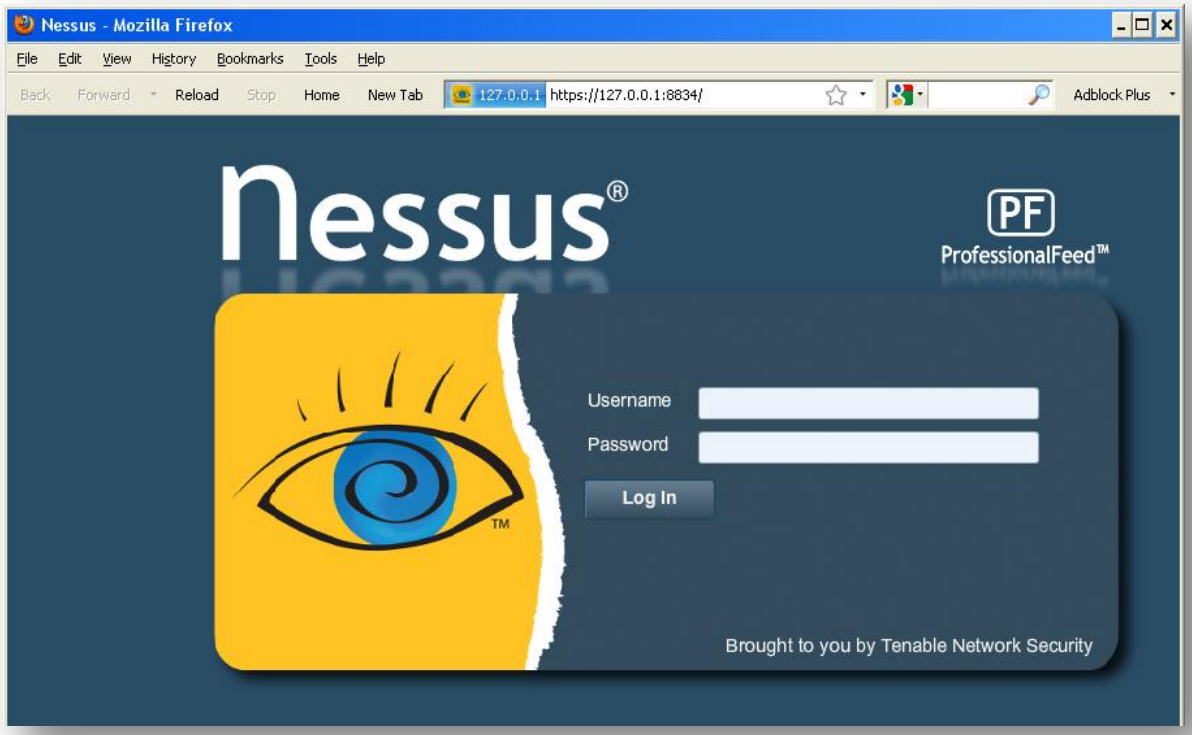

This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.0.2:8834, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

Benutzer von Microsoft Internet Explorer können auf „Continue to this website (not recommended“ (Laden dieser Website fortsetzen (nicht empfohlen) klicken, um die Nessus-Benutzeroberfläche zu laden. Benutzer von Firefox 3.x-10.x klicken auf „I Understand the Risks“ (Ich kenne das Risiko) und dann auf „Add Exception...“ (Ausnahme hinzufügen…), um das Dialogfeld „Add Security Exception“ (Sicherheits-Ausnahmeregel hinzufügen) aufzurufen:


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
https://192.168.0.2:8834/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

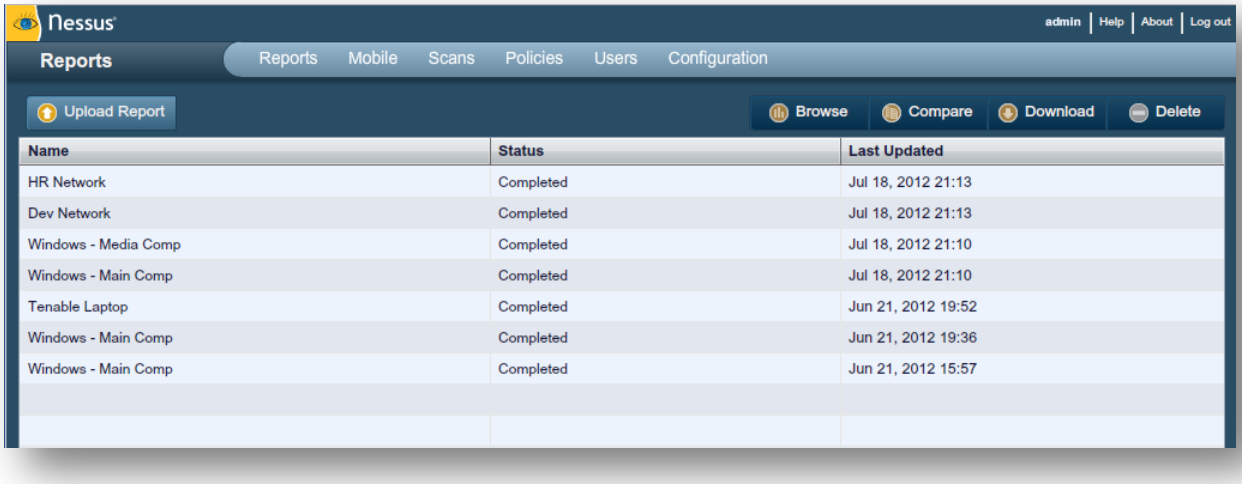
Vergewissern Sie sich, dass im Feld „Location:“ (Adresse) die URL des Nessus-Servers steht, und klicken Sie auf „**Confirm Security Exception**“ (Sicherheits-Ausnahmeregel bestätigen). Weitere Informationen zur Installation eines angepassten SSL-Zertifikats entnehmen Sie dem Nessus-Installations- und Konfigurationshandbuch.

Nachdem die Ausnahme in Ihrem Browser bestätigt wurde, wird das folgende Startfenster angezeigt:

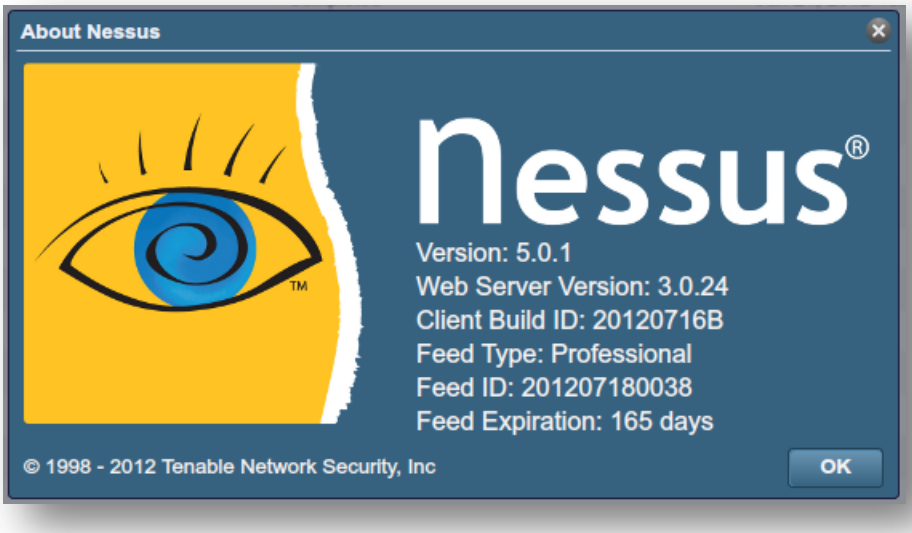


Auf dem Startbildschirm ist angegeben, ob Nessus gegenwärtig für einen HomeFeed oder einen ProfessionalFeed registriert ist:

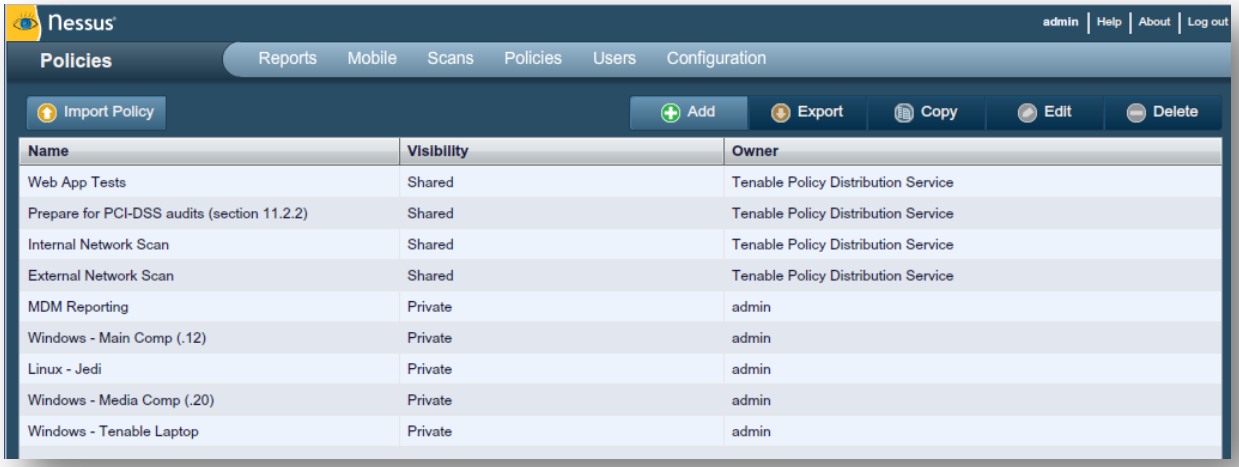
Authentifizieren Sie sich mithilfe des Benutzernamens und des Kennworts, das Sie während des Installationsvorgangs erstellt haben. Nach erfolgreicher Authentifizierung erscheinen auf der Benutzeroberfläche die Menüs zum Erstellen von Richtlinien, zum Durchführen von Scans und zum Suchen von Berichten:


Nessus
admin | Help | About | Log out
Reports
Reports Mobile Scans Policies Users Configuration
Upload Report
Browse Compare Download Delete
Name Status Last Updated
HR Network Completed Jul 18, 2012 21:13
Dev Network Completed Jul 18, 2012 21:13
Windows - Media Comp Completed Jul 18, 2012 21:10
Windows - Main Comp Completed Jul 18, 2012 21:10
Tenable Laptop Completed Jun 21, 2012 19:52
Windows - Main Comp Completed Jun 21, 2012 19:36
Windows - Main Comp Completed Jun 21, 2012 15:57

Die oben rechts gezeigten Optionen sind zu jedem Zeitpunkt der Benutzung von Nessus verfügbar. Die Angabe „admin“, die oben rechts in der oben gezeigten Abbildung zu sehen ist, nennt das Konto, unter dem Sie sich angemeldet haben. Wenn Sie darauf klicken, können Sie Ihr aktuelles Kennwort ändern. „Help“ („Hilfe“) ist eine Verknüpfung mit der Nessus-Dokumentation, die ausführliche Hinweise zur Verwendung der Software enthält. „About“ („Info“) zeigt wichtige Informationen zur Nessus-Installation an, z. B. Version, Typ und Ablauf des Feeds, den Client-Build und die Webserverversion. „Log out“ („Abmelden“) beendet Ihre aktuelle Sitzung.



Überblick zu den Richtlinien


Nessus
admin | Help | About | Log out
Policies
Reports Mobile Scans Policies Users Configuration
Import Policy
Add Export Copy Edit Delete
Name Visibility Owner
Web App Tests Shared Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2) Shared Tenable Policy Distribution Service
Internal Network Scan Shared Tenable Policy Distribution Service
External Network Scan Shared Tenable Policy Distribution Service
MDM Reporting Private admin
Windows - Main Comp (.12) Private admin
Linux - Jedi Private admin
Windows - Media Comp (.20) Private admin
Windows - Tenable Laptop Private admin

Eine Nessus-Richtlinie umfasst Konfigurationsoptionen für die Durchführung von Sicherheitslückenscans. Hierzu zählen unter anderem:

- Parameter zur Steuerung technischer Aspekte des Scans (z. B. Timeouts, Anzahl der Hosts, Art des Portscanners usw.)
- Anmeldedaten für lokale Scans (z. B. Windows, SSH), authentifizierte Oracle-Datenbankscans, HTTP, FTP, POP, IMAP oder eine Kerberos-basierte Authentifizierung
- Spezifikationen für abgestufte Scans auf Basis von Plugins oder Plugin-Familien.
- Tests der Compliancerichtlinien für Datenbanken, Ausführlichkeit von Berichten, Scaneinstellungen für die Diensterkennung, UNIX-Compliancetests u. a.

Standardrichtlinien

Nessus
Policies
Reports Mobile Scans Policies Users Configuration
Import Policy
Add Export Copy
Name Visibility Owner
Web App Tests Shared Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2) Shared Tenable Policy Distribution Service
Internal Network Scan Shared Tenable Policy Distribution Service
External Network Scan Shared Tenable Policy Distribution Service

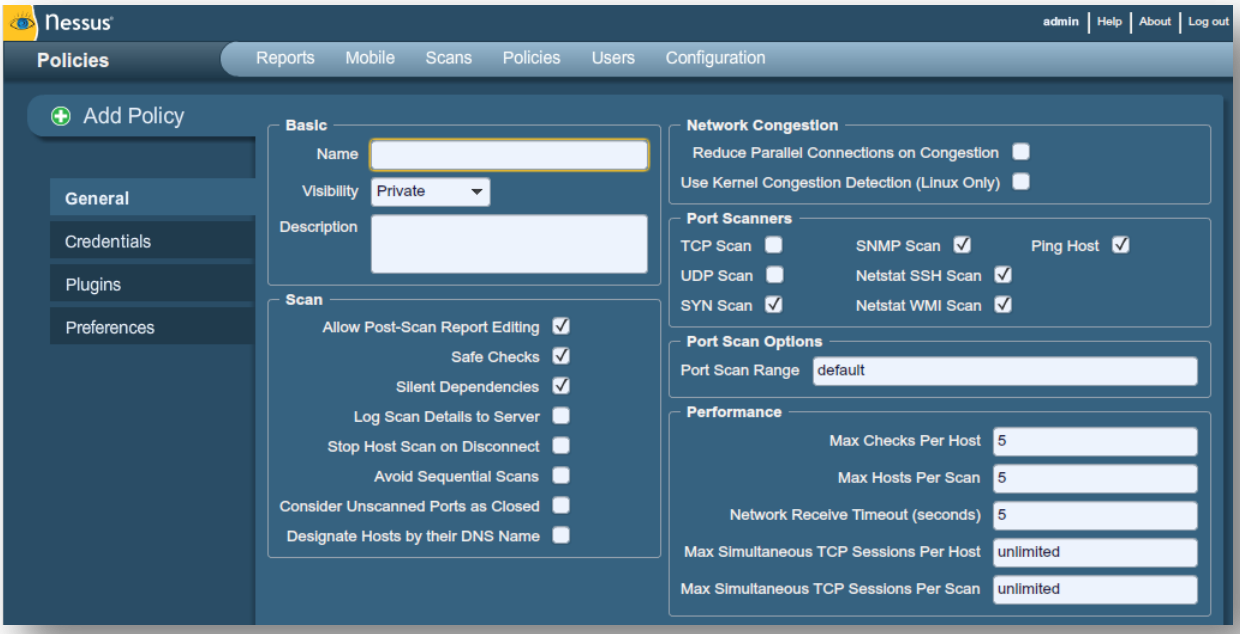
Nessus wird mit einer Reihe von Standardrichtlinien ausgeliefert, die von Tenable Network Security, Inc. bereitgestellt werden. Sie dienen einerseits als Vorlagen, auf deren Basis Sie angepasste Richtlinien für Ihre Organisation erstellen können, können aber auch direkt zur Ausführung einfacher Scans Ihrer Ressourcen verwendet werden. Machen Sie sich mit den Standardrichtlinien vertraut, bevor Sie Ihre Ressourcen damit scannen.

Name der Richtlinie	Beschreibung
External Network Scan (Externer Netzwerkscan)	Diese Richtlinie dient dem Scannen von Hosts, die mit Ressourcen außerhalb Ihres Netzwerks verbunden sind. Solche Hosts stellen gewöhnlich weniger Dienste in Ihrem Netzwerk bereit. In dieser Richtlinie sind Plugins aktiviert, die bekannte Sicherheitslücken von Webanwendungen überprüfen (es sind dies die Plugin-Familien „CGI Abuses“ und „CGI Abuses: XSS“). Außerdem werden alle 65.536 Ports (einschließlich Port 0 über ein separates Plugin) auf jedem Ziel gescannt.
Internal Network Scan (Interner Netzwerkscan)	Diese Richtlinie dient der Leistungsoptimierung. Bei der Erstellung wurde berücksichtigt, dass sie zum Scannen umfangreicher interner Netzwerke mit vielen Hosts, mehreren ungeschützten Diensten und eingebetteten Systemen wie etwa Druckern verwendet werden kann. Die CGI-Tests sind hier deaktiviert, und es werden statt aller 65.535 nur häufig verwendete Ports gescannt.
Web App Tests (Web-App-Tests)	Wenn Sie Ihre Systeme scannen möchten und Nessus sowohl bekannte als auch unbekannte Sicherheitslücken in Ihren Webanwendungen erkennen soll, ist dies die passende Scanrichtlinie für Sie. Die unscharfen Suchfunktionen in Nessus sind in dieser Richtlinie aktiviert. Aufgrund dessen sucht Nessus auf allen erkannten Websites nach Sicherheitslücken in allen Parametern einschließlich XSS, SQL, Befehlsinjektion usw. Mit dieser Richtlinie werden Probleme über HTTP und HTTPS erkannt.
Prepare for PCI DSS audits (Für PCI-DSS-Tests vorbereiten)	Diese Richtlinie aktiviert die integrierten PCI-DSS-Compliancetests, bei denen Scanergebnisse mit den PCI-Standards verglichen werden und ein Bericht zum Complianceniveau erstellt wird. Es ist sehr wichtig festzuhalten, dass ein erfolgreicher Compliancescan weder Compliance noch eine sichere Infrastruktur garantiert. Organisationen, bei denen eine PCI-DSS-Bewertung ansteht, können ihr Netzwerk und ihre Systeme mithilfe dieser Richtlinie auf die PCI-DSS-Compliance vorbereiten.

Wenn Sie eine von Tenable bereitgestellte Standardrichtlinie als Grundlage für ihre eigene benutzerdefinierte Richtlinie nutzen möchten, verwenden Sie die Kopierfunktion. Wenn Sie eine Standardrichtlinie bearbeiten, werden Sie selbst zum Besitzer der Richtlinie, und sie erscheint nicht mehr auf der Benutzeroberfläche.

Neue Richtlinie erstellen

Wenn Sie eine Verbindung mit einer Nessus-Serverbenutzeroberfläche hergestellt haben, können Sie eine angepasste Richtlinie erstellen. Hierzu klicken Sie auf die Option „**Policies**“ („Richtlinien“) oben in der Menüleiste und dann rechts auf die Schaltfläche „**+ Add**“ („Hinzufügen“). Das Fenster „**Add Policy**“ („Richtlinie hinzufügen“) erscheint:



Hier finden Sie vier Registerkarten für die Konfiguration: **General** („Allgemein“), **Credentials** („Anmeldedaten“), **Plugins** und **Preferences** („Einstellungen“). Die Standardeinstellungen ermöglichen eine maximal abgestufte Kontrolle des Nessus-Scannerbetriebs und müssen für die meisten Umgebungen nicht geändert werden. Die Registerkarten sind nachfolgend beschrieben.

Allgemein

Die Registerkarte „**General**“ erlaubt das Benennen der Richtlinie und die Konfiguration scanspezifischer Vorgänge. Hier finden Sie sechs Bereiche mit zusammengefassten Optionen, die das Scannerverhalten steuern:

Im Bereich „**Basic**“ („Grundlagen“) definieren Sie Aspekte zur Richtlinie selbst:

Option	Beschreibung
Name	Hier wird der Name festgelegt, der zur Bezeichnung der Richtlinie auf der Nessus-Benutzeroberfläche verwendet wird.
Visibility (Sichtbarkeit)	Hierdurch wird bestimmt, ob die Richtlinie mit anderen Benutzern gemeinsam verwendet wird („*Shared*“) oder Ihrem persönlichen Gebrauch vorbehalten bleibt („*Private*“). Nur Administratoren können Richtlinien zur gemeinsamen Verwendung freigeben.
Description (Beschreibung)	Hier kann eine kurze Beschreibung der Scanrichtlinie eingegeben werden. Das Feld eignet sich normalerweise zur Zusammenfassung des allgemeinen Zwecks der Richtlinie (z. B. „Webserverscans ohne lokale Tests und Nicht-HTTP-Dienste“).

Im Bereich „**Scan**“ werden die weiteren Optionen in Zusammenhang mit dem Verhalten eines Scans definiert:

Option	Beschreibung
Allow Post-Scan Report Editing (Nachträgliche Bearbeitung von Berichten gestatten)	Mithilfe dieser Funktion kann der Benutzer Elemente aus dem Bericht löschen. Wenn ein Scan auf Einhaltung gesetzlicher Vorschriften oder sonstiger Vorgaben (Compliance) durchgeführt wird, darf diese Option nicht ausgewählt werden, damit nachgewiesen werden kann, dass der Scan nicht manipuliert wurde.
Safe Checks (Sichere Tests)	„Safe Checks“ deaktiviert alle Plugins, die sich unter Umständen negativ auf den Remotehost auswirken können.
Silent Dependencies (Abhängigkeiten nicht aufführen)	Wenn diese Option aktiviert ist, wird die Liste der Abhängigkeiten nicht im Bericht aufgeführt. Soll die Liste der Abhängigkeiten im Bericht enthalten sein, dann müssen Sie das Kontrollkästchen deaktivieren.
Log Scan Details to Server (Scandetails auf Server protokollieren)	Hiermit werden zusätzliche Details des Scans in der Nessus-Serverlogdatei (`nessusd.messages`) gespeichert, z. B. der Start, die Beendigung oder der erzwungene Abbruch von Plugins. Anhand der resultierenden Logdatei können Sie nachprüfen, ob bestimmte Plugins verwendet und Hosts gescannt wurden.
Stop Host Scan on Disconnect (Hostscan bei Trennung beenden)	Wenn diese Option aktiviert ist, beendet Nessus den Scan, sobald erkannt wurde, dass der Host nicht mehr reagiert. Dies kann beispielsweise geschehen, wenn Benutzer den PC während eines Scans abschalten, ein Host nach Verwendung eines Denial-of-Service-Plugins nicht mehr reagiert oder ein Sicherheitsmechanismus (z. B. ein IDS) die Datenübertragung an den Server gesperrt hat. Würde der Scan solcher Computer fortgesetzt, so würde unnötiger Datenverkehr im Netzwerk übertragen, und der Scan würde verzögert.
Avoid Sequential Scans (Fortlaufende Scans vermeiden)	Standardmäßig scannt Nessus eine Liste mit IP-Adressen in fortlaufender Reihenfolge. Wenn jedoch diese Option aktiviert ist, scannt Nessus die Liste in zufälliger Reihenfolge. Dies ist normalerweise nützlich, um den an ein bestimmtes Subnetz gerichteten Datenverkehr besser zu verteilen, wenn der Scan umfangreich ist.
Consider Unscanned Ports as Closed (Nicht gescannte Ports als geschlossen betrachten)	Wenn ein Port mit einem ausgewählten Portscanner nicht gescannt wird (weil er beispielsweise außerhalb des angegebenen Bereichs liegt), wird er von Nessus als geschlossen betrachtet.
Designate Hosts by their DNS Name (DNS-Namen für Hosts)	Wenn Sie diese Option auswählen, wird statt der IP-Adresse der Hostname in der Berichtsausgabe verwendet.

Im Bereich „**Network**“ finden Sie Optionen, mit denen sich die Steuerung des Scans in Bezug auf das zu scannende Zielnetzwerk optimieren lässt:

Option	Beschreibung
Reduce Parallel Connections on Congestion (Parallele Verbindungen bei Überlast verringern)	Bei Aktivierung dieser Option kann Nessus erkennen, dass zu viele Pakete versendet werden und die maximale Kapazität der Netzwerkverbindung in Kürze erreicht werden wird. In diesem Fall drosselt Nessus die Scanrate, um die Überlastung zu mindern. Nach Minderung der Überlastung versucht Nessus automatisch, die verfügbare Kapazität der Netzwerkverbindung wieder optimal zu nutzen.

Use Kernel Congestion Detection (Kernel-Überlastungserkennung verwenden, nur Linux)	Ermöglicht Nessus die Überwachung der CPU und anderer interner Vorgänge auf Überlastung und eine ggf. erforderliche Verringerung der Verarbeitungsgeschwindigkeit. Nessus wird immer versuchen, möglichst alle verfügbaren Ressourcen zu verwenden. Diese Funktionalität ist nur für Nessus-Scanner verfügbar, die auf einem Linux-System installiert sind.

Im Bereich „**Port Scanners**“ („Portscanner“) legen Sie fest, welche Methoden für das Scannen von Ports aktiviert werden sollen:

Option	Beschreibung
TCP Scan	Verwendet den integrierten TCP-Scanner von Nessus zur Ermittlung offener TCP-Ports auf den Zielsystemen. Dieser Scanner ist optimiert und verfügt über Selbstoptimierungsfunktionen. Auf einigen Plattformen (z. B. Windows oder Mac OS X) wird bei Auswahl dieses Scanners der SYN-Scanner verwendet, um schwerwiegende Leistungsprobleme zu vermeiden, die für die betreffenden Betriebssysteme spezifisch sind.
UDP Scan	Verwendet den integrierten UDP-Scanner von Nessus zur Ermittlung offener UDP-Ports auf den Zielsystemen. UDP ist ein „zustandsloses“ Protokoll, d. h. die Kommunikation erfolgt nicht über Handshake-Dialoge. Die UDP-basierte Kommunikation ist nicht immer zuverlässig und aufgrund der Eigenschaften von UDP-Diensten und -Auslesegeräten auch nicht immer remote erkennbar.
SYN Scan	Verwendet den integrierten SYN-Scanner von Nessus zur Ermittlung offener TCP-Ports auf den Zielsystemen. SYN-Scans sind ein beliebter Ansatz zur Durchführung von Portscans und gelten im Vergleich zu TCP-Scans allgemein als weniger aggressiv. Der Scanner sendet ein SYN-Paket an diesen Port, wartet auf die SYN-ACK-Antwort und bestimmt den Portstatus anhand der Antwort bzw. anhand des Ausbleibens der Antwort.
SNMP Scan	Hiermit wird Nessus angewiesen, Ziele auf das Vorhandensein eines SNMP-Diensts zu prüfen. Nessus versucht während eines SNMP-Scans, relevante Einstellungen zu erschließen. Wenn die Einstellungen durch den Benutzer unter „Preferences“ angegeben wurden, kann Nessus den Remotehost besser testen und ausführlichere Auditresultate generieren. Beispielsweise gibt es eine ganze Reihe von Tests für Cisco-Router, mit denen durch Verarbeitung des zurückerhaltenen SNMP-Strings die vorhandenen Sicherheitslücken ermittelt werden. Diese Angaben sind für solche Audits erforderlich.
Netstat SSH Scan	Diese Option nutzt **`netstat`** zur Überprüfung offener Ports auf dem lokalen Computer. Hierzu wird auf den Befehl **`netstat`** zurückgegriffen, der über eine SSH-Verbindung zum Ziel verfügbar ist. Der Scan ist in erster Linie für Systeme auf UNIX-Basis gedacht und erfordert Anmeldedaten zur Authentifizierung.
Netstat WMI Scan	Diese Option nutzt **`netstat`** zur Überprüfung offener Ports auf dem lokalen Computer. Hierzu wird auf den Befehl **`netstat`** zurückgegriffen, der über eine WMI-Verbindung zum Ziel verfügbar ist. Der Scan ist in erster Linie für Windows-Systeme gedacht und erfordert Anmeldedaten zur Authentifizierung.

	Ein Scan auf WMI-Basis ermittelt mithilfe von **`netstat`** offene Ports, d. h. angegebene Portbereiche werden ignoriert. Wenn ein Port-Enumerator (**`netstat`** oder SNMP) erfolgreich ist, umfasst der Portbereich nachfolgend alle Ports (Einstellung „all“). Allerdings wird Nessus die Option „Consider Unscanned Ports As Closed“ (Nicht gescannte Ports als geschlossen betrachten) berücksichtigen, sofern diese ausgewählt ist.
Ping Host (Pingbefehl an Host senden)	Diese Option ermöglicht das Senden von Pingbefehlen an Remotehosts über mehrere Ports, um festzustellen, ob sie online sind.

Über den Bereich „**Port Scan Options**“ („Optionen für Portscans“) wird ein bestimmter Portbereich als Zielbereich festgelegt. Die folgenden Werte sind für die Option „Port Scan Range“ („Portscanbereich“) zulässig:

Wert	Beschreibung
„default“ (Standard)	Wenn das Schlüsselwort „default“ angegeben wird, scannt Nessus ca. 4.790 häufig verwendete Ports. Die Liste dieser Ports kann der Datei **`nessus-services`** entnommen werden.
„all“ (Alle)	Wenn das Schlüsselwort „all“ angegeben wird, scannt Nessus alle 65.535 Ports.
Custom List (Benutzerdefinierte Liste)	Ein benutzerdefinierter Portbereich kann mithilfe einer Liste durch Kommata getrennter Ports oder Portbereiche festgelegt werden. Beispielsweise sind Angaben wie „21,23,25,80,110“ oder „1-1024,8080,9000-9200“ zulässig. Wenn Sie „1-65535“ festlegen, werden alle Ports gescannt. Sie können auch einen Teilbereich angeben, der für das jeweilige Protokoll spezifisch ist. Wenn Sie beispielsweise mithilfe derselben Richtlinie unterschiedliche Portbereiche für TCP und UDP scannen möchten, könnten Sie Folgendes angeben:„T:1-1024,U:300-500“. Des Weiteren können Sie eine Gruppe von Ports, die für beide Protokolle gescannt werden sollen, und zusätzlich Einzelbereiche für das jeweilige Protokoll angeben (z. B. „1-1024,T:1024-65535,U:1025“). Wenn Sie nur ein einziges Protokoll scannen, wählen Sie lediglich den betreffenden Portscanner aus und geben Sie die Ports wie üblich an.

Der für einen Portscan angegebene Bereich ist gleichermaßen für TCP- und UDP-Scans gültig.

Im Bereich „**Performance**“ sind zwei Optionen vorhanden, mit denen die Anzahl der zu startenden Scans gesteuert wird. Diese Optionen sind bei der Konfiguration eines Scans die vielleicht wichtigsten, denn sie haben die stärksten Auswirkungen auf Scandauer und Netzwerkaktivitäten.

Option	Beschreibung
Max Checks Per Host (Tests je Host maximal)	Mit dieser Einstellung wird die Anzahl der Tests begrenzt, die ein Nessus-Scanner gleichzeitig für einen einzelnen Host ausführt.
Max Hosts Per Scan (Hosts je Scan maximal)	Mit dieser Einstellung wird die Anzahl der Hosts begrenzt, die von einem Nessus-Scanner gleichzeitig gescannt werden.

Network Receive Timeout (Timeout für Netzwerkdatenempfang, in Sekunden)	Der Standardwert liegt bei fünf Sekunden. Es handelt sich um die Zeit, für die Nessus auf eine Antwort von einem Host wartet (sofern durch ein Plugin nichts anderes festgelegt ist). Wenn Sie über eine langsame Verbindung scannen, sollten Sie hier einen höheren Wert eingeben.
Max Simultaneous TCP Sessions Per Host (Gleichzeitige Anzahl TCP-Sitzungen je Host maximal)	Durch diese Einstellung kann die Anzahl gleichzeitig laufender TCP-Sitzungen für einen einzelnen Host beschränkt werden. Mithilfe dieser TCP-Drosselung steuern Sie auch die Anzahl der Pakete, die der SYN-Scanner letztendlich pro Sekunde sendet (ist diese Option beispielsweise auf 15 festgelegt, dann sendet der SYN-Scanner maximal 1500 Pakete pro Sekunde).
Max Simultaneous TCP Sessions Per Scan (Gleichzeitige Anzahl TCP-Sitzungen je Scan maximal)	Durch diese Einstellung kann die Anzahl gleichzeitig laufender TCP-Sitzungen für den gesamten Scan beschränkt werden (die Anzahl der gescannten Hosts spielt hierbei keine Rolle). Bei Nessus-Scannern, die unter Windows XP, Vista oder 7 installiert sind, darf dieser Wert höchstens 19 betragen, da andernfalls keine korrekten Resultate zu erzielen sind.

Credentials

Auf der nachfolgend abgebildeten Registerkarte „**Credentials**“ (Anmeldedaten) können Sie die Verwendung von Authentifizierungsdaten für Scanvorgänge durch den Nessus-Scanner konfigurieren. Nach der Konfiguration dieser Informationen kann Nessus eine größere Zahl von Tests ausführen und gelangt so zu genaueren Ergebnissen.

Im Dropdownmenü „**Windows credentials**“ („Windows-Anmeldedaten“) sind Einstellungen enthalten, um Nessus Informationen wie den Namen, das Kennwort und den Domänennamen für das SMB-Konto zu übermitteln. SMB (Server Message Block) ist ein Dateifreigabeprotokoll, mit dem Computer Daten im gesamten Netzwerk transparent verwenden können. Mithilfe dieser Angaben kann Nessus lokale Daten über einen Windows-Remotehost suchen. Beispielsweise kann Nessus unter Verwendung der Authentifizierungsdaten feststellen, ob wichtige Sicherheitspatches bereits aufgespielt wurden. Die Standardwerte der anderen SMB-Parameter müssen nicht geändert werden.

Sind mehrere SMB-Konten konfiguriert, probiert Nessus die angegebenen Anmeldedaten bis zur erfolgreichen Anmeldung nacheinander aus. Nach erfolgreicher Authentifizierung mit einem Satz Anmeldedaten prüft Nessus auch die übrigen angegebenen Anmeldedaten, verwendet sie aber nur, wenn diese Administratorzugriff gewähren, während die vorherigen Konten lediglich einen Benutzerzugriff gestatten.

Einige Windows-Versionen lassen die Einrichtung eines neuen Kontos mit Designierung als „Administrator“ zu. Für authentifizierte Scans sind diese Konten jedoch nicht unbedingt geeignet. Tenable empfiehlt, dass Sie für authentifizierte Scans das ursprüngliche Administratorkonto mit der Bezeichnung „Administrator“ verwenden, um vollen Zugriff zu erhalten. Bei bestimmten Windows-Versionen ist dieses Konto möglicherweise ausgeblendet. Das eigentliche Administratorkonto lässt sich einblenden, indem Sie das DOS-Prompt mit Administratorrechten öffnen und diesen Befehl eingeben:

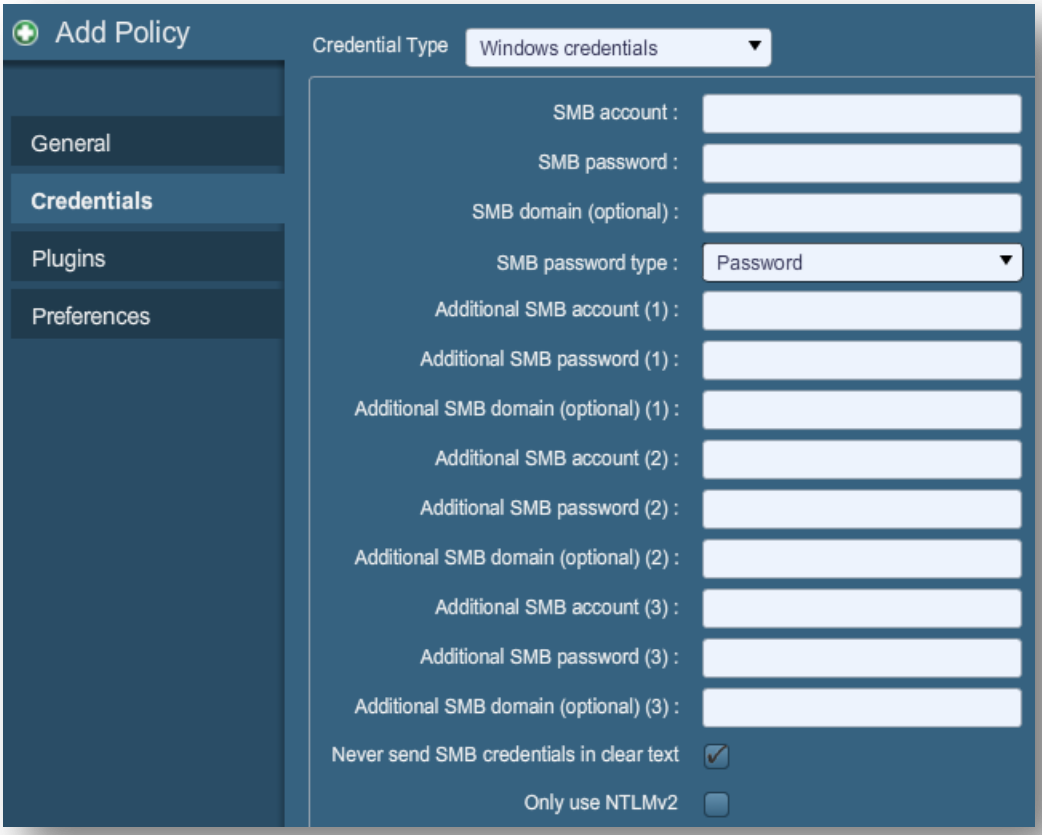
```
C:\> net user administrator /active:yes
```

Wenn ein SMB-Wartungskonto mit eingeschränkten Administratorrechten erstellt wird, kann Nessus mehrere Domänen einfach und sicher scannen.

Tenable empfiehlt Netzwerkadministratoren die Erstellung bestimmter Domänenkonten, um Tests zu vereinfachen. Nessus umfasst eine Vielzahl von Sicherheitstests für Windows NT, 2000, Server 2003, XP, Vista, Windows 7 und

Windows 2008, die genauer arbeiten, wenn ein Domänenkonto angegeben wird. Allerdings versucht Nessus in den meisten Fällen, verschiedene Tests auch ohne Kontenangabe auszuführen.

Der Windows-Dienst „Remote-Registrierung“ ermöglicht Remotecomputern mit entsprechenden Anmeldedaten den Zugriff auf die Registrierung des überprüften Computers. Wird der Dienst nicht ausgeführt, dann ist das Auslesen von Schlüsseln und Werten aus der Registrierung auch bei Angabe gültiger Authentifizierungsdaten nicht möglich. Weitere Informationen entnehmen Sie dem Tenable-Blogbeitrag „Dynamic Remote Registry Auditing - Now you see it, now you don’t!“. Dieser Dienst **muss für einen authentifizierten** Nessus Scan ausgeführt werden, um ein System unter Einsatz der Anmeldedaten vollständig zu prüfen.



Nach der Auswahl von „**SSH settings**“ („SSH-Einstellungen“) aus dem Dropdownmenü und der Eingabe von Anmeldedaten können UNIX-Systeme ausgewählt werden. Diese Anmeldedaten werden verwendet, um für Patchaudits oder Compliancetests lokale Informationen von UNIX-Remotesystemen abzurufen. Es sind Felder für die Eingabe des SSH-Benutzernamens für das Konto, unter dem die Tests auf dem UNIX-Zielsystem ausgeführt werden, sowie für das SSH-Kennwort oder das SSH-Schlüsselpaar (öffentlicher und geheimer Schlüssel) vorhanden. In ein weiteres Feld können Sie ggf. die Passphrase für den SSH-Schlüssel eingeben.

Nessus 4 unterstützt die Verschlüsselungsalgorithmen **`blowfish-cbc`**, **`aes-cbc`** und **`aes-ctr`**.

Die wirksamsten authentifizierten Scans sind solche, bei denen das angegebene Konto über Root-Berechtigungen verfügt. Da zahlreiche Sites eine Remoteanmeldung als Root nicht zulassen, können Nessus-Benutzer „**`su`**“, „**`sudo`**“,

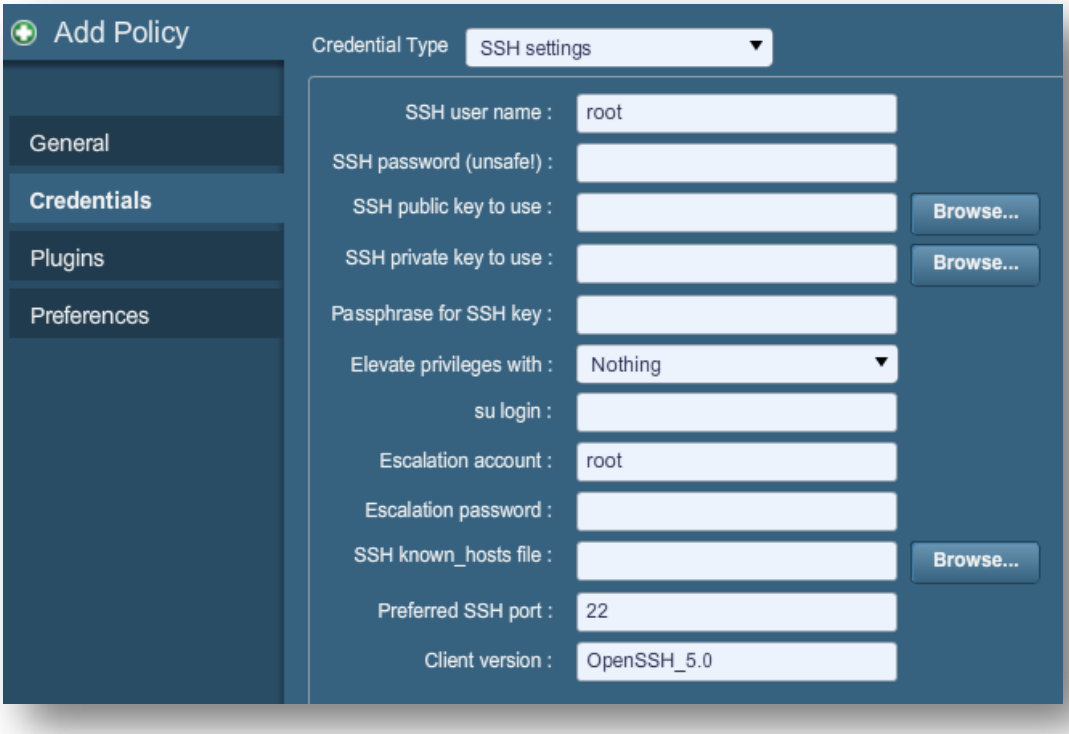
„**su+sudo**“ oder „**dzdo**“ mit einem separaten Kennwort für ein Konto aufrufen, für das „**su**“- oder „**sudo**“-Berechtigungen konfiguriert wurden. Außerdem kann Nessus Berechtigungen auf Cisco-Geräten eskalieren, wenn „**Cisco 'enable'**“ ausgewählt wird.

Nessus kann zur Authentifizierung bei einem Remoteserver einen Zugriff auf SSH-Basis verwenden. Wenn die SSH-Datei „**known_hosts** “ vorhanden und als Teil der Scanrichtlinie angegeben ist, wird Nessus sich, sofern möglich, nur bei den in dieser Datei genannten Hosts anmelden. Schließlich kann unter „Preferred SSH port“ noch der bevorzugte SSH-Port festgelegt werden, falls Nessus die Verbindung mit SSH über einen anderen als den Standardport 22 herstellen soll.

Nessus verschlüsselt alle in den Richtlinien gespeicherten Kennwörter. Allerdings sehen die Best Practices vor, zur Authentifizierung SSH-Schlüssel anstelle von SSH-Kennwörtern zu verwenden. Auf diese Weise soll sichergestellt werden, dass mithilfe des Benutzernamens und des Kennworts, die Sie für Audits Ihrer bekannten SSH-Server verwenden, kein Anmeldeversuch auf einem System vorgenommen wird, das sich nicht unter ihrer Kontrolle befindet. Aufgrund dessen wird zur Verwendung von SSH-Kennwörtern nur dann geraten, wenn es absolut unabdingbar ist.

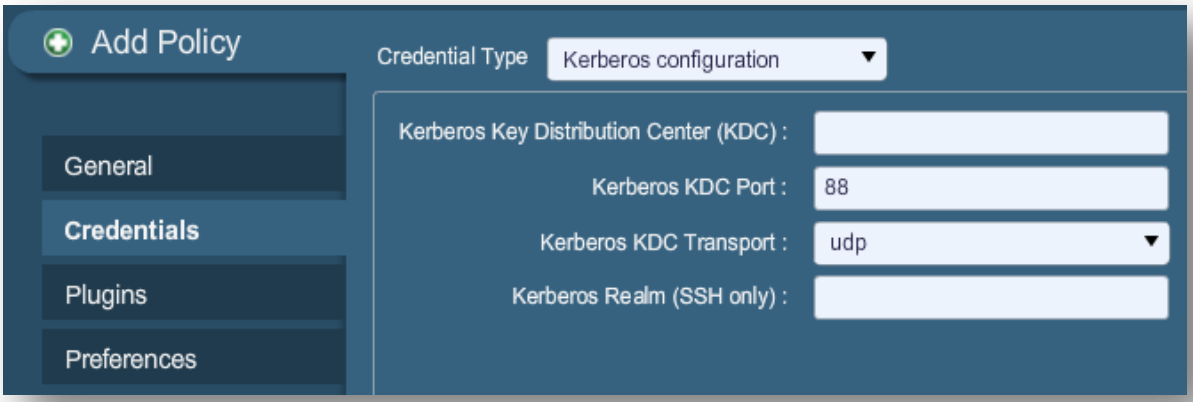
Nessus unterstützt auch eine Option „su+sudo“. Diese kann verwendet werden, falls ein System keine Berechtigungen für die Remoteanmeldung berechtigter Konten gestattet.

Die folgende Bildschirmabbildung zeigt die verfügbaren SSH-Optionen. Das Dropdownmenü „Elevate privileges with“ („Berechtigungen hochstufen mit“) enthält verschiedene Methoden zum Hochstufen von Berechtigungen nach erfolgreicher Authentifizierung.

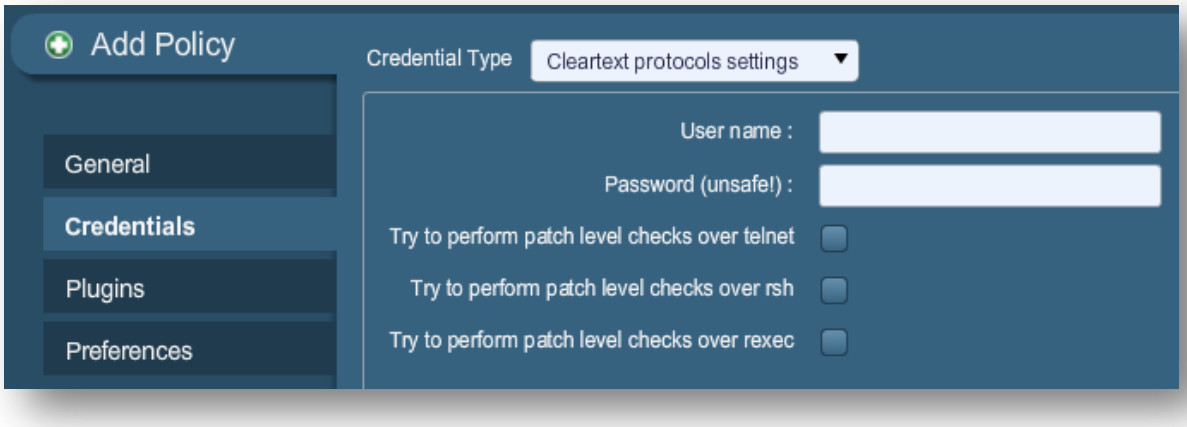


Wenn zur Eskalation von Berechtigungen ein anderes Konto als **root** verwendet werden muss, kann dieses unter „**Escalation account**“ („Eskalationskonto“) und das zugehörige Kennwort unter „**Escalation password**“ („Eskalationskennwort“) angegeben werden.

Mit „**Kerberos configuration**“ („Kerberos-Konfiguration“) können Sie Anmeldedaten unter Verwendung von Kerberos-Schlüsseln von einem Remotesystem aus angeben:



Schließlich kann, wenn eine sichere Methode zur Durchführung authentifizierter Tests nicht verfügbar ist, der Versuch erzwungen werden, Nessus-Tests über unsichere Protokolle durchzuführen. Hierzu muss das Element „**Cleartext protocol settings**“ („Einstellungen für unverschlüsselte Protokolle“) im Dropdownmenü konfiguriert werden. Unterstützt werden für diese Option die unverschlüsselten Protokolle **telnet**, **rsh** und **rexec**.



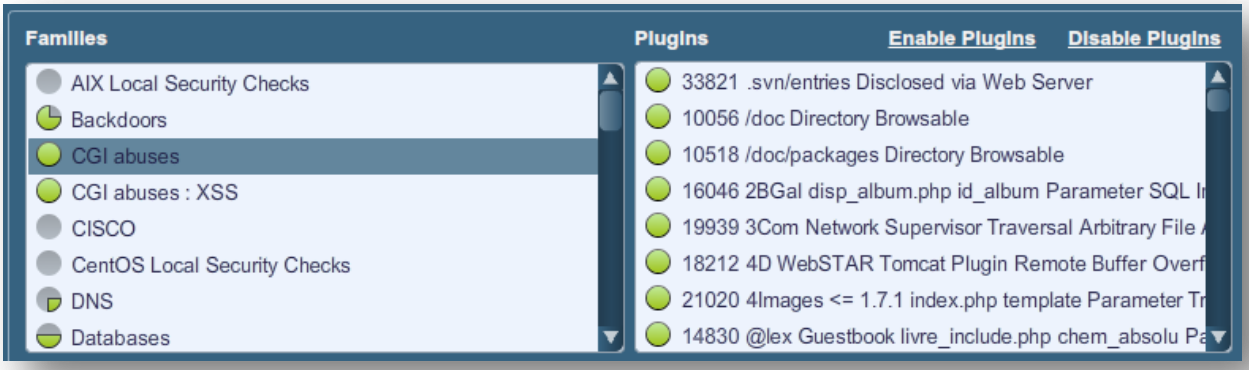
Standardmäßig sind alle Kennwörter (und auch die Richtlinie selbst) verschlüsselt. Wird die Richtlinie in einer `.nessus`-Datei gespeichert und diese Datei nachfolgend auf eine andere Nessus-Installation kopiert, dann sind die Kennwörter für den zweiten Nessus-Scanner unzugänglich, da er sie nicht entschlüsseln kann.

Von der Verwendung unverschlüsselter Authentifizierungsdaten wird **dringend** abgeraten! Werden die Anmeldedaten remote (z. B. bei einem Nessus-Scan) übermittelt, dann können sie von jeder Person abgefangen werden, die Zugriff auf das Netzwerk hat. Deswegen sollten Sie, sofern dies irgendwie möglich ist, Mechanismen zur verschlüsselten Authentifizierung verwenden.

Plugins

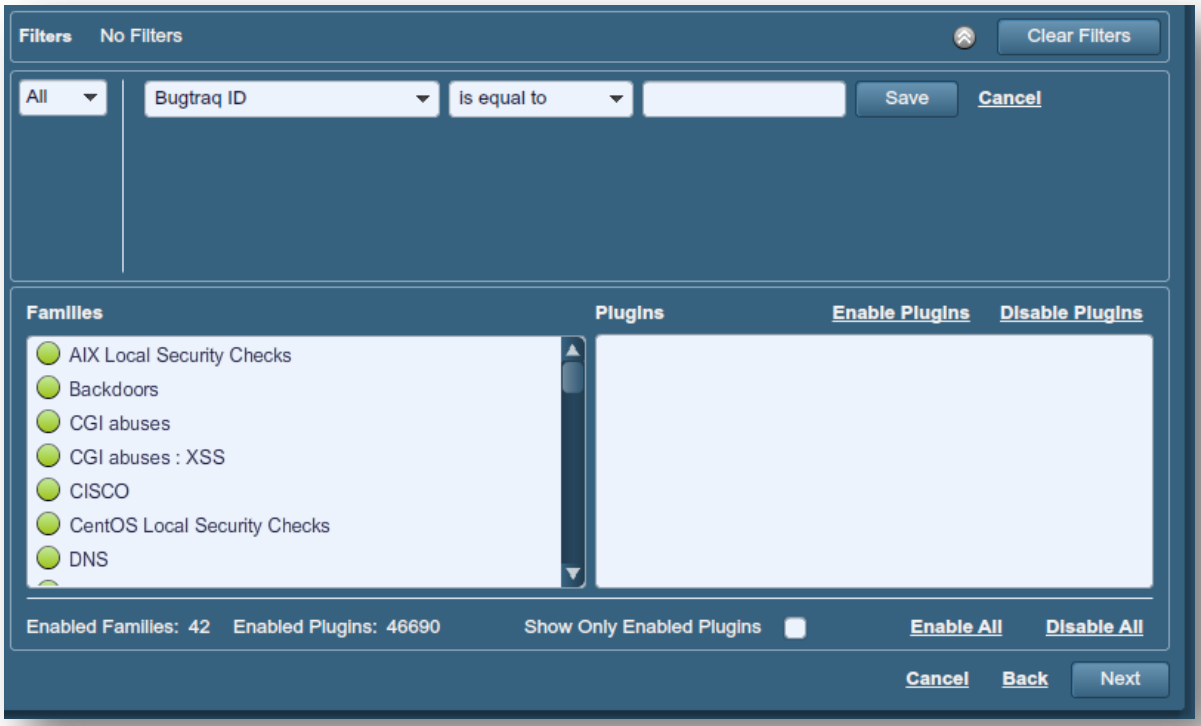
Die Registerkarte „**Plugins**“ ermöglicht die Auswahl bestimmter Sicherheitstests durch Plugin-Familien wie auch einzelne Tests.

Durch Anklicken des gelben Kreises neben einer Plugin-Familie können Sie die gesamte Familie aktivieren (grün) oder deaktivieren (grau). Bei Auswahl einer Familie wird die Liste der zugehörigen Plugins in der oberen rechten Ecke angezeigt. Einzelne Plugins können separat aktiviert oder deaktiviert werden, um die Scanrichtlinien exakt für den eigenen Bedarf maßzuschneidern. Während Sie die Einstellungen vornehmen, werden die Gesamtzahlen der ausgewählten Familien und Plugins unten im Fenster angezeigt. Wenn der Kreis neben einer Plugin-Familie zu 25, 50 oder 75 Prozent grün ist, weist dies darauf hin, dass nicht alle, sondern nur die entsprechende Anzahl Plugins aktiviert sind.

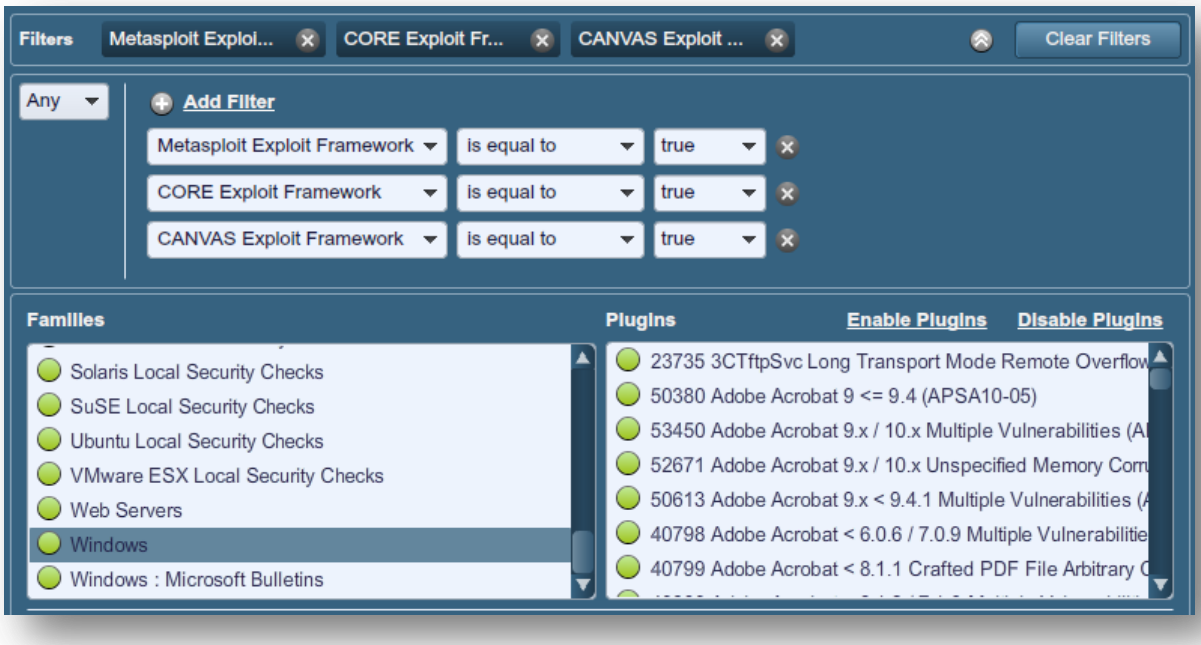


Bei Auswahl eines Plugins wird dessen Ausgabe so angezeigt, wie sie später in einem Bericht enthalten sein wird. Die Zusammenfassung und die Beschreibung enthalten weitere Details zur untersuchten Sicherheitslücke. Wenn Sie im Bereich „Plugin Description“ („Plugin-Beschreibung“) nach unten blättern, erscheinen auch Hinweise zur Behebung, ggf. weitere Verweise und die CVSSv2-Bewertung (mit dieser wird eine allgemeine Risikobewertung angegeben).

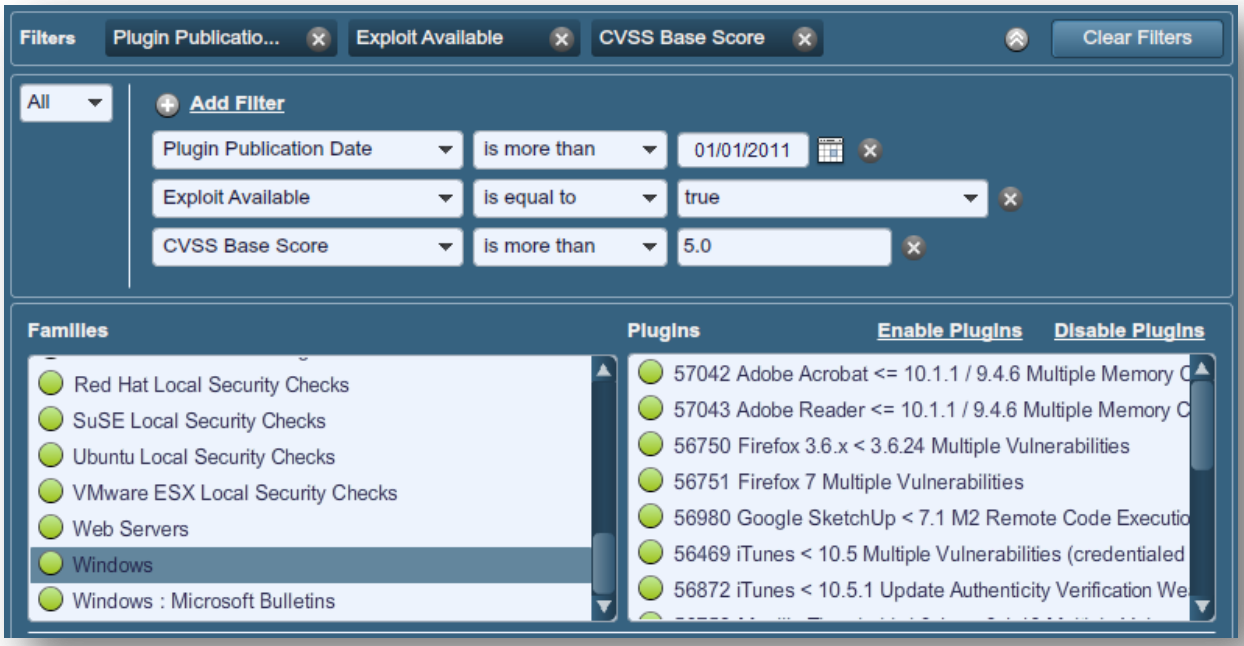
Oben auf der Registerkarte mit den Plugin-Familien können Sie Filter erstellen und so eine Liste mit Plugins einrichten, die Bestandteil der Richtlinie werden. Filter ermöglichen eine fein abgestufte Plugin-Auswahl. Für eine Richtlinie können mehrere Filter festgelegt sein. Zum Erstellen eines Filters klicken Sie auf den Link „**Add Filter**“ („Filter hinzufügen“):



Jeder Filter bietet Ihnen verschiedene Optionen, um die Suche zu verfeinern. Für die Anwendung der Filterkriterien stehen Ihnen die Optionen „Any“ („Beliebige“), bei der bereits bei Erfüllung mindestens eines Kriteriums ein Ergebnis zurückgegeben wird, und „All“ („Alle“) zur Verfügung, bei der alle Filterkriterien vorhanden sein müssen. Wenn Sie beispielsweise eine Richtlinie nur mit solchen Plugins erstellen möchten, für die in einem kommerziellen Exploit-Framework ein Exploit vorhanden ist, können Sie drei Filter erstellen und für die Kriterienanwendung „Any“ auswählen:



Möchten Sie eine Richtlinie mit Plugins erstellen, die mehreren Kriterien entsprechen, dann wählen Sie „All“ aus und fügen die gewünschten Filter hinzu. Die nachfolgende Richtlinie beispielsweise würde alle nach dem ersten Januar 2011 veröffentlichten Plugins enthalten, für die ein öffentlicher Exploit vorhanden ist und die eine CVSS-Basisbewertung von mehr als 5.0 aufweisen:



Eine vollständige Liste der Filterkriterien und zugehörigen Parameter finden Sie im Abschnitt „Berichtsfilter“ des vorliegenden Dokuments.

Zur Erstellung von Richtlinien mithilfe von Filtern wird empfohlen, zunächst alle Plugins zu deaktivieren. Ermitteln Sie die Plugins, die Bestandteil der Richtlinie werden sollen, dann mithilfe von Plugin-Filtern. Wenn Sie fertig sind, wählen Sie die einzelnen Plugin-Familien aus und klicken auf „Enable Plugins“ („Plugins aktivieren“).

Wenn eine Richtlinie erstellt und gespeichert wird, sind in ihr alle Plugins vermerkt, die ursprünglich ausgewählt wurden. Wenn neue Plugins über ein Plugin-Feedupdate empfangen werden, werden diese automatisch aktiviert, sofern die zugehörige Familie in der Richtlinie bereits aktiviert ist. Wurde die Familie vollständig oder teilweise deaktiviert, dann werden auch neue Plugins dieser Familie automatisch deaktiviert.

Die Familie „Denial of Service“ enthält einige Plugins, die in einem Netzwerk Ausfälle verursachen können, wenn die Option „Safe Checks“ deaktiviert ist; auf der anderen Seite enthält sie auch einige nützliche Tests, die keinen Schaden anrichten können. Sie können die Familie „Denial of Service“ in Verbindung mit der aktivierten Option „Safe Checks“ verwenden, um sicherzustellen, dass potenziell gefährliche Plugins nicht ausgeführt werden. Wir empfehlen allerdings, die Familie „Denial of Service“ in einem Produktionsnetzwerk nicht einzusetzen.

Unter dem Fenster, dass die Plugins auflistet, befinden sich drei Optionen, die Ihnen bei Auswahl und Anzeige der Plugins behilflich sein werden.

Option	Beschreibung
Show Only Enabled Plugins (Nur aktivierte Plugins anzeigen)	Wenn Sie diese Option auswählen, zeigt Nessus nur Plugins an, die – wahlweise manuell oder über einen Filter – ausgewählt wurden.
Enable all (Alle aktivieren)	Hiermit werden alle Plugins und ihre Familien ausgewählt und aktiviert. Es handelt sich hierbei um eine einfache Möglichkeit, alle Plugins zu reaktivieren, wenn Sie zuvor eine Richtlinie erstellt haben, in der einige Familien oder Plugins deaktiviert wurden. Beachten Sie, dass für einige Plugins weitere Optionen konfiguriert werden müssen.
Disable all (Alle deaktivieren)	Hiermit werden alle Plugins und ihre Familien abgewählt und deaktiviert. Wenn Sie einen Scan ausführen, bei dem alle Plugins deaktiviert sind, werden keine Ergebnisse generiert.

Preferences

Die Registerkarte „**Preferences**“ („Voreinstellungen“) enthält Optionen für eine fein abgestufte Steuerung der Scanrichtlinieneinstellungen. Bei Auswahl eines Elements aus dem Dropdownmenü werden weitere Konfigurationselemente für die betreffende Kategorie angezeigt. Beachten Sie, dass die Liste der Konfigurationsoptionen dynamisch ist, d. h. sie hängt vom Plugin-Feed, von den Auditrichtlinien und weiteren Funktionen ab, auf die der verbundene Nessus-Scanner zugreifen kann. Bei einem Scanner mit einem ProfessionalFeed stehen unter Umständen mehr fortgeschrittene Konfigurationsoptionen zur Verfügung als bei einem Scanner, für den der HomeFeed konfiguriert wurde. Außerdem ändert sich diese Liste, wenn Plugins hinzugefügt oder geändert werden.

Die folgende Liste bietet eine Übersicht über alle Einstellungen. Ausführlichere Informationen zu den einzelnen Parametern entnehmen Sie dem Abschnitt Details zu Scaneinstellungen im vorliegenden Dokument.

Einstellung	Beschreibung
ADSI settings (ADSIEinstellungen)	Active Directory Service Interfaces (ADSI oder Serviceoberfläche des Active Directory) ruft Informationen vom Mobile Device Management (MDM)-Server in Bezug auf Android- und iOS-basierte Geräte ab.
Apple Profile Manager API Settings (API-Einstellungen des Apple Profile Managers)	Eine ProfessionalFeed-Funktion, die die Enumeration und Scans auf Sicherheitslücken für Apple iOS-Geräte wie iPhone, iPad usw. aktiviert.
Cisco IOS Compliance Checks (Cisco IOS-Compliancetests)	Option für den ProfessionalFeed, die die Angabe einer Richtliniendatei zum Testen von Cisco IOS-Geräten auf die Einhaltung von Compliancestandards gestattet.
Database Compliance Checks (Datenbank-Compliancetests)	Option für den ProfessionalFeed, die die Angabe einer Richtliniendatei zum Testen von Datenbanken wie DB2, SQL Server, MySQL und Oracle auf die Einhaltung von Compliancestandards gestattet.
Database Settings (Datenbankeinstellungen)	Optionen zur Angabe des zu testenden Datenbanktyps und der zu verwendenden Anmeldedaten.
Do not scan fragile devices (Anfällige Geräte nicht scannen)	Mithilfe dieser Optionen weisen Sie Nessus an, bestimmte Geräte **nicht** zu scannen, weil ein erhöhtes Risiko besteht, die Zielgeräte zum Absturz zu bringen.
Global variable settings (Einstellungen globaler Variablen)	Zahlreiche Optionen für die Nessus-Konfiguration.

HTTP cookies import (HTTP-Cookies importieren)	Beim Testen von Webanwendungen wird mit dieser Option eine externe Datei angegeben, in die HTTP-Cookies importiert werden, um eine Authentifizierung bei der Anwendung zu gestatten.
HTTP login page (HTTP-Anmeldeseite)	Einstellungen, die sich auf die Anmeldeseite bei Webanwendungstests beziehen.
IBM iSeries Compliance Checks (Compliancetests für IBM iSeries-Systeme)	Option für den ProfessionalFeed, die die Angabe einer Richtliniendatei zum Testen von IBM iSeries-Systemen auf die Einhaltung von Compliancestandards gestattet.
IBM iSeries Credentials (Anmeldedaten für IBM iSeries)	Bezeichnet den Speicherort der Anmeldedaten für IBM iSeries-Systeme.
ICCP/COTP TSAP Addressing Weakness (Adressierungsschwächen)	Option für den ProfessionalFeed im Zusammenhang mit SCADA-Tests (Supervisory Control And Data Acquisition).
Login configurations (Anmeldekonfigurationen)	Bezeichnet den Speicherort, an dem Anmeldedaten für einfache HTTP-, NNTP-, FTP-, POP- und IMAP-Diensttests abgelegt sind.
Modbus/TCP Coil Access (Modbus/TCP Coil-Zugriff)	Option für den ProfessionalFeed im Zusammenhang mit SCADA-Tests (Supervisory Control And Data Acquisition).
Nessus SYN scanner (Nessus SYN-Scanner)	Optionen für den integrierten SYN-Scanner.
Nessus TCP scanner (Nessus TCP-Scanner)	Optionen für den integrierten TCP-Scanner.
News Server (NNTP) Information Disclosure (NNTP-Datenenthüllung)	Optionen zum Testen von NNTP-Servern auf bestimmte Sicherheitslücken, durch die Daten enthüllt werden könnten.
Oracle Settings (Oracle-Einstellungen)	Optionen für Tests von Oracle-Datenbankinstallationen.
PCI DSS Compliance (PCI-DSS-Compliance)	Option für den ProfessionalFeed, die einen Abgleich der Scanergebnisse mit den PCI-DSS-Standards startet.
Patch Management: Red Hat Satellite Server Settings (Patchmanagement: Einstellungen für Red Hat-Satellite-Server)	Optionen für die Integration von Nessus mit dem Red Hat-Satellite-Patchmanagementserver. Weitere Informationen entnehmen Sie dem Dokument Patch Management Integration.
Patch Management: SCCM Server Settings (Patchmanagement: Einstellungen für SCCM-Server)	Optionen für die Integration von Nessus mit dem SCCM-Patchmanagementserver (System Center Configuration Manager). Weitere Informationen entnehmen Sie dem Dokument Patch Management Integration.
Patch Management: VMware Go Server Settings (Patchmanagement: Einstellungen für VMware Go Server)	Optionen für die Integration von Nessus mit dem VMware Go Server (vormals Shavlik). Weitere Informationen entnehmen Sie dem Dokument Patch Management Integration.
Patch Management: WSUS Server Settings (Patchmanagement: Einstellungen für WSUS-Server)	Optionen für die Integration von Nessus mit dem WSUS-Patchmanagementserver (Windows Server Update Service). Weitere Informationen entnehmen Sie dem Dokument Patch Management Integration.

Ping the remote host (Pingbefehl an Remotehost senden)	Mit diesen Einstellungen steuert Nessus die Ping-basierte Netzwerkerkennung.
Port scanner settings (Einstellungen für Portscanner)	Zwei Einstellungen, die die Steuerung von Portscanaktivitäten verbessern.
SMB Registry: Start the Registry Service during the scan (SMB-Registrierung: Registrierungsdienst bei laufendem Scan starten)	Hiermit wird Nessus angewiesen, den SMB-Registrierungsdienst auf Hosts zu starten, auf denen er nicht aktiviert ist.
SMB Scope (SMB-Umfang)	Weist Nessus an, Domänenbenutzer anstelle lokaler Benutzer abzufragen.
SMB Use Domain SID to Enumerate Users (SMB: Domänen-SID für Benutzeraufzählung verwenden)	Mit dieser Option können Sie den SID-Bereich für SMB-Lookups von Domänenbenutzern angeben.
SMB Use Host SID to Enumerate Local Users (SMB: Host-SID für Aufzählung lokaler Benutzer verwenden)	Mit dieser Option können Sie den SID-Bereich für SMB-Lookups lokaler Benutzer angeben.
SMTP Settings (SMTP-Einstellungen)	Optionen für SMTP-Tests (Simple Mail Transport Protocol).
SNMP Settings (SNMP-Einstellungen)	Konfigurations- und Authentifizierungsdaten für SNMP (Simple Network Management Protocol).
Service Detection (Diensterkennung)	Mit diesen Optionen werden Tests SSL-basierter Dienste gesteuert.
Unix Compliance Checks (UNIX-Compliancetests)	Option für den ProfessionalFeed, die die Angabe einer Richtliniendatei zum Testen von UNIX-Systemen auf die Einhaltung von Compliancestandards gestattet.
VMware SOAP API Settings (Einstellungen für VMware-SOAP-API)	Konfigurations- und Authentifizierungsdaten für die SOAP-API von VMware.
Wake-on-LAN (WOL)	Hiermit wird Nessus angewiesen, vor der Durchführung eines Scans Wake-on-LAN-Pakete zu senden.
Web Application Test Settings (Einstellungen für Webanwendungstests)	Optionen für Tests von Webanwendungen.
Web mirroring (Web-Mirroring)	Konfigurationsdetails zur Steuerung der Anzahl von Webseiten, die von Nessus gespiegelt werden, um die Inhalte auf Sicherheitslücken zu prüfen.
Windows Compliance Checks (Windows-Compliancetests)	Option für den ProfessionalFeed, die die Angabe einer Richtliniendatei zum Testen von Windows-Systemen auf die Einhaltung von Compliancestandards gestattet.
Windows File Contents Compliance Checks (Windows-Compliancetests für Dateiinhalte)	Option für den ProfessionalFeed, die die Angabe einer Richtliniendatei zum Testen von Dateien auf Windows-Systemen auf die Einhaltung von Compliancestandards gestattet.

Aufgrund aktualisierter XML-Metadaten in Nessus 5 stehen mit Nessus 4 generierte Compliancedaten im Abschnitt „Compliance Checks“ exportierter Berichte nicht mehr zur Verfügung. Allerdings sind die Compliancedaten auf der Nessus-Weboberfläche ersichtlich.

Richtlinien importieren, exportieren und kopieren

Über die Schaltfläche „**Import**“ oben links können Sie zuvor erstellte Richtlinien in den Scanner hochladen. Wählen Sie über das Dialogfeld „**Browse…**“ („Durchsuchen“) die Richtlinie auf Ihrem lokalen System aus und klicken Sie auf „**Submit**“ („Absenden“).

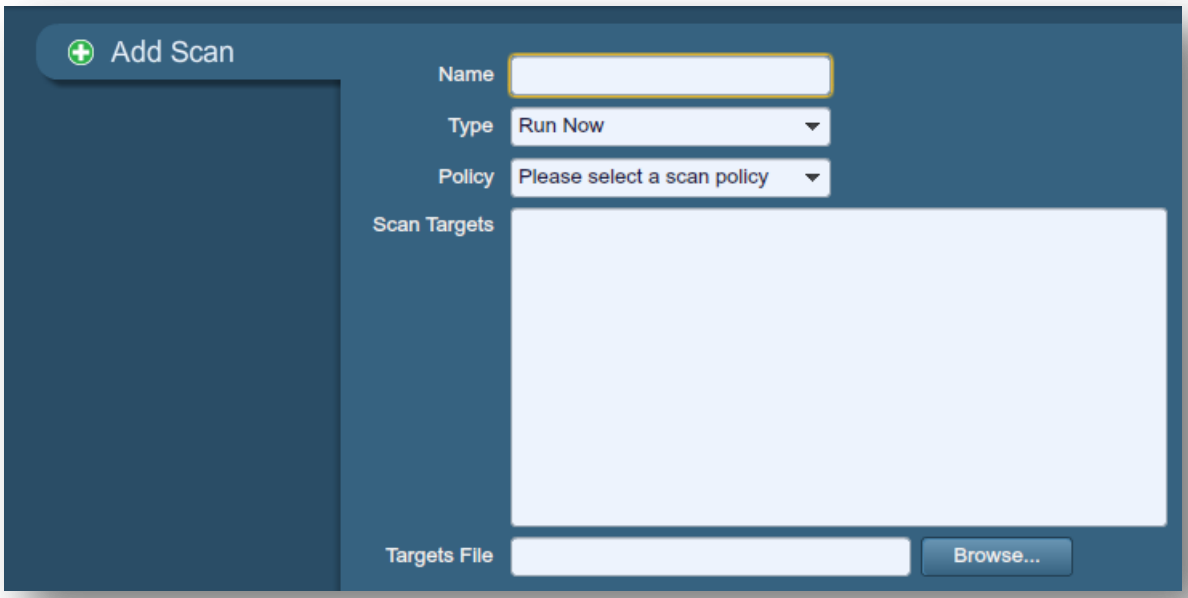
Über die Schaltfläche „**Export**“ in der Menüleiste können Sie eine bestehende Richtlinie aus dem Scanner auf das lokale Dateisystem herunterladen. Im Downloaddialogfeld des Browsers können Sie angeben, dass die Richtlinie in einem externen Programm (z. B. dem Texteditor) geöffnet oder in einem frei wählbaren Verzeichnis gespeichert wird.

Kennwörter und `.audit`-Dateien, die in einer Richtlinie enthalten sind, werden **nicht** exportiert.

Wenn Sie eine Richtlinie erstellen möchten, die im Vergleich zu einer vorhandenen Richtlinie nur kleinere Änderungen aufweist, können Sie die Ausgangsrichtlinie in der Liste auswählen und dann oben rechts in der Menüleiste auf „**Copy**“ („Kopieren“) klicken. Hierdurch wird eine Kopie der Ausgangsrichtlinie erstellt, die bearbeitet werden kann, um die erforderlichen Änderungen vorzunehmen. Dies ist sinnvoll zur Erstellung von Standardrichtlinien mit geringfügigen Änderungen, wie sie für die gegebene Umgebung erforderlich sind.

Scans erstellen, starten und planen

Wenn Sie eine Richtlinie erstellt haben, können Sie einen neuen Scan anlegen. Hierzu klicken Sie auf die Option „**Scans**“ oben in der Menüleiste und dann rechts auf die Schaltfläche „**+ Add**“ („Hinzufügen“). Das Fenster „**Add Scan**“ („Scan hinzufügen“) erscheint:



Hier sind fünf Felder zur Eingabe des Scanziels vorhanden:

- **Name**: Hier wird der Name festgelegt, der zur Bezeichnung des Scans auf der Nessus-Benutzeroberfläche verwendet wird.
- **Type** (Typ): Wählen Sie „Run Now“ („Jetzt ausführen“; führt den Scan unmittelbar nach der Eingabe aus), „Scheduled“ („Geplant“; erlaubt die Festlegung des Zeitpunkts, zu dem der Scan gestartet werden soll) oder „Template“ („Vorlage“; speichert die Eingaben als Vorlage für wiederholbare Scans).
- **Policy** (Richtlinie): Wählen Sie eine zuvor erstellte Richtlinie aus, anhand derer die Parametereinstellungen für den Scan vorgenommen werden. Mit diesen wird das Verhalten des Nessus-Serverscanners kontrolliert.

- **Scan Targets** (Scanziele): Ziele können als einzelne IP-Adresse (z. B. „192.168.0.1“), als IP-Bereich (z. B. „192.168.0.1-192.168.0.255“), als Subnetz in CIDR-Notation (z. B. „192.168.0.0/24“) oder als auflösbarer Host (z. B. „www.nessus.org“) angegeben werden.
- **Targets File** (Zieldatei): Eine Textdatei, die eine Liste mit Hosts enthält, kann durch Anklicken von „**Browse…**“ und nachfolgende Auswahl einer Datei auf dem lokalen Computer importiert werden.

Die Hostdatei muss als ASCII-Text formatiert sein. Pro Zeile muss ein Host angegeben sein, und es dürfen weder Leerzeichen noch Leerzeilen vorhanden sein. Die Unicode-/UTF-8-Kodierung wird nicht unterstützt.

Beispiel für Hostdateiformate:

Einzelne Hosts:

192.168.0.100
192.168.0.101
192.168.0.102

Hostbereich:

192.168.0.100-192.168.0.102

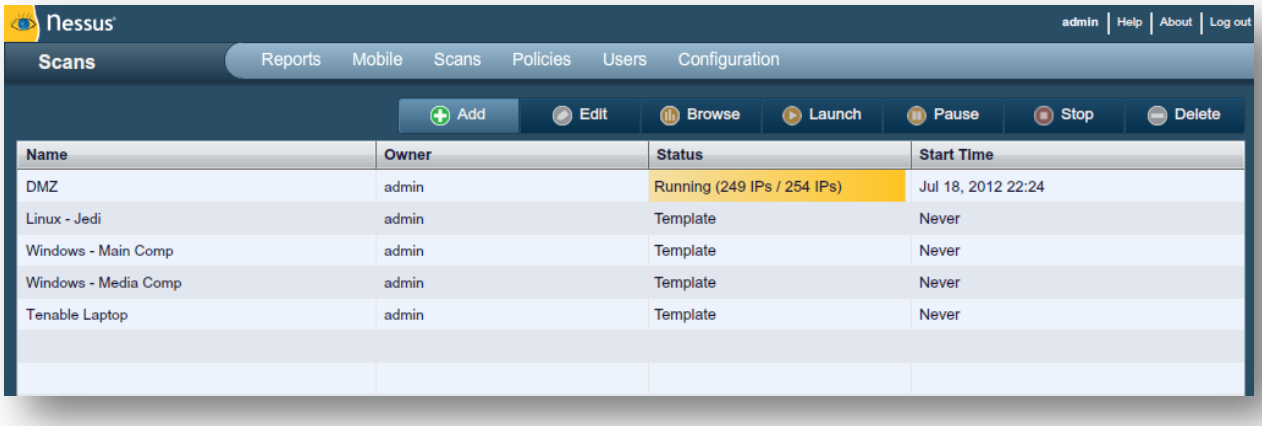
Hostblock in CIDR-Notation:

192.168.0.1/24

Virtuelle Server:

www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]

Klicken Sie nach Angabe der Scaninformationen auf „**Submit**“ (Absenden). Nach der Übertragung beginnt der Scan sofort, sofern Sie zuvor „Run Now“ (Jetzt ausführen) ausgewählt haben. Erst nach Abschluss des Scans wird wieder die allgemeine Seite „**Scans**“ angezeigt.

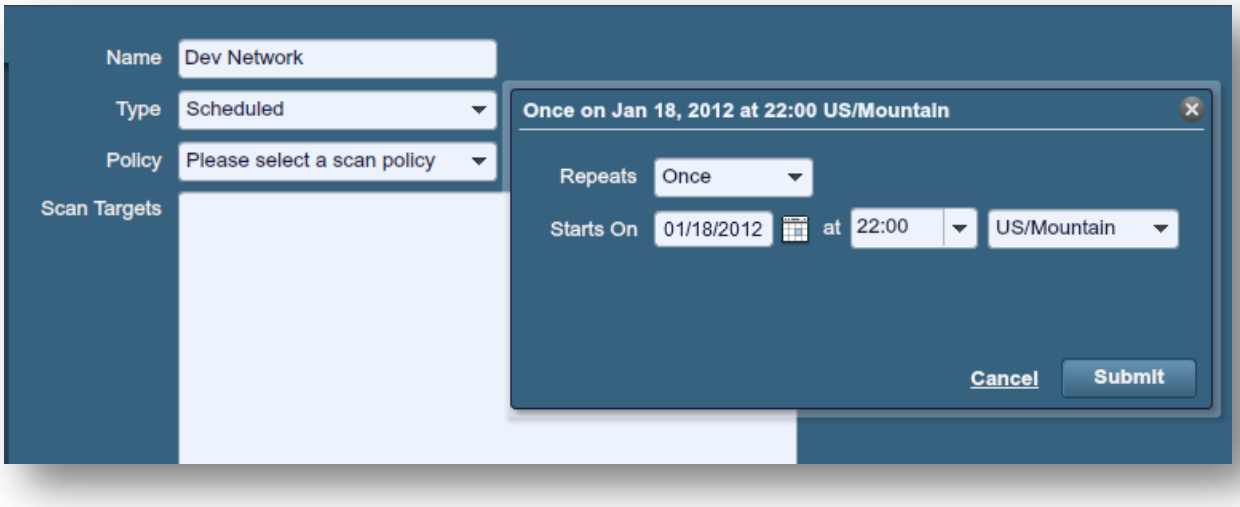


Nach dem Starten des Scans zeigt die Liste „Scans“ alle gegenwärtig laufenden, unterbrochenen oder als Vorlage ausgewählten Scans sowie zugehörige Basisinformationen an. Nach Auswählen eines bestimmten Scans aus der Liste können Sie über die Schaltflächen oben rechts die laufenden Scanergebnisse durchsuchen („**Browse**“), den Scan

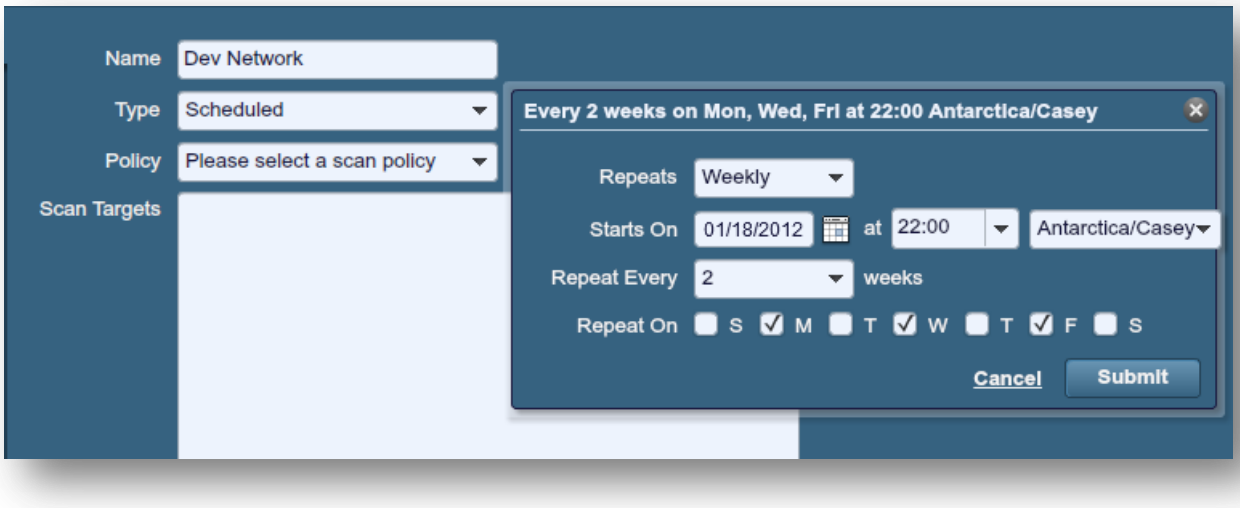
unterbrechen („**Pause**“) und fortsetzen („**Resume**“), ihn beenden („**Stop**“) und bei Bedarf vollständig löschen („**Delete**“). Außerdem können Benutzer Scanvorlagen nach Anklicken der Schaltfläche „**Edit**“ bearbeiten.

Wenn ein Scan (auf welche Weise auch immer) beendet wurde, wird er aus der Liste „**Scans**“ entfernt. Gleichzeitig wird er zur Kontrolle auf der Registerkarte „**Reports**“ hinzugefügt.

Wurde ein Scan geplant („Scheduled“), dann werden Optionen zur Eingabe der gewünschten Startzeit und der Häufigkeit angezeigt:

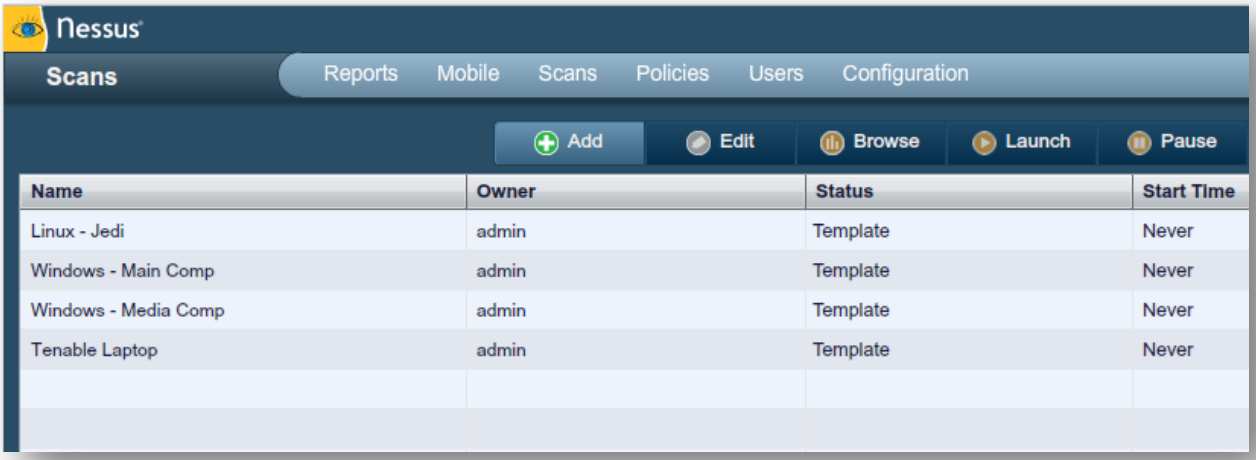


Über das Dropdownmenü „Repeats“ („Wiederholungen“) können Sie festlegen, ob ein Scan einmalig, täglich, wöchentlich, monatlich oder jährlich ausgeführt wird. Für die hier getroffene Auswahl kann zudem ein Startzeitpunkt (Datum und Uhrzeit) festgelegt werden. Ist der Scan gespeichert, dann wird er von Nessus zum gewünschten Zeitpunkt gestartet.



Die Möglichkeit der Zeitplanung von Scans steht nur ProfessionalFeed-Kunden zur Verfügung.

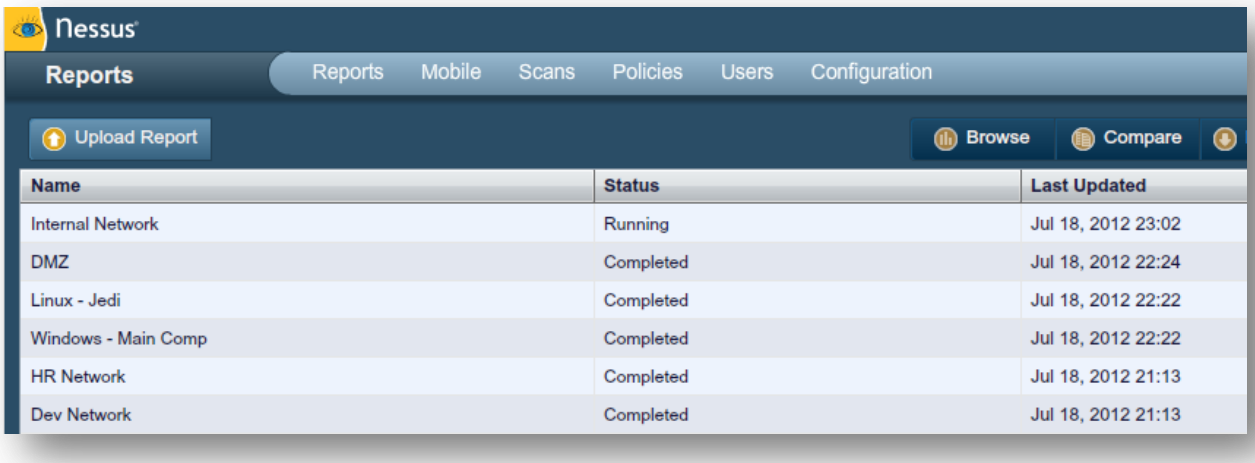
Wurde ein Scan als Vorlage gespeichert, dann wird er in der Scanliste auch als solche angezeigt und kann gestartet werden.



Berichte

Beginnend mit Nessus 5 können Benutzer eigene Berichte erstellen, die verschiedene Kapitel aufweisen: „Vulnerability Centric“ („sicherheitslückenzentrisch“), „Host Centric“ („hostzentrisch“), „Compliance“ und „Compliance Executive“. Das HTML-Format wird standardmäßig weiterhin unterstützt; ist allerdings Java auf dem Scannerhost installiert, dann können Berichte auch im PDF-Format exportiert werden. Mithilfe von Berichtsfiltern und Exportfunktionen kann der Benutzer dynamische Berichte auf der Basis der eigenen Prioritäten erstellen, statt lediglich aus einer Liste vorgefertigter Berichte auszuwählen.

Wenn Sie oben auf der Benutzeroberfläche auf die Registerkarte „**Reports**“ („Berichte“) klicken, wird eine Liste mit laufenden und abgeschlossenen Scans angezeigt:

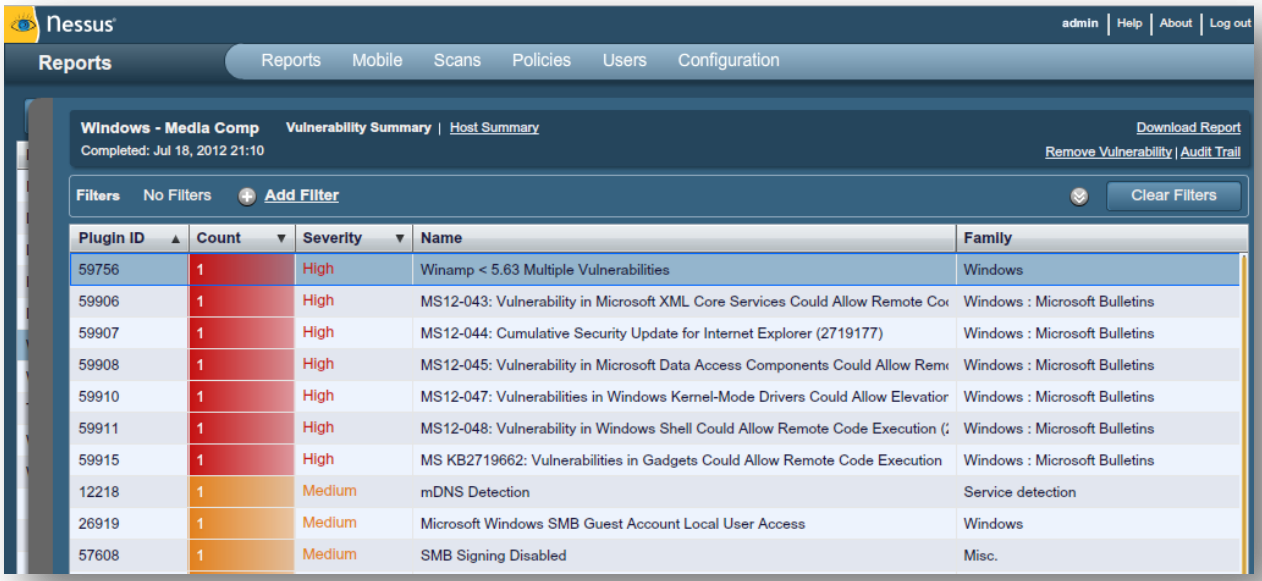


Der Bildschirm „**Reports**“ („Berichte“) ist die zentrale Anlaufstelle zum Anzeigen, Vergleichen, Hochladen und Herunterladen von Scanergebnissen. Mithilfe der Umschalt- oder der STRG-Taste können Sie mehrere Berichte gleichzeitig auswählen.

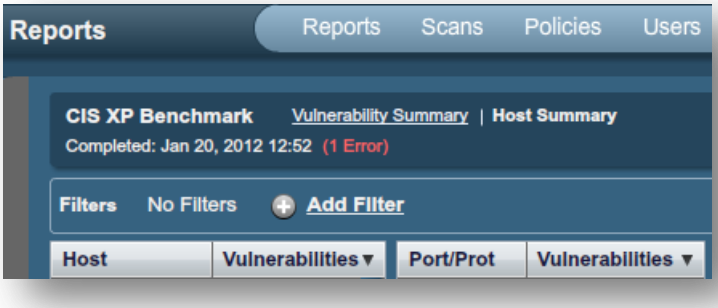
Browse (Durchsuchen)

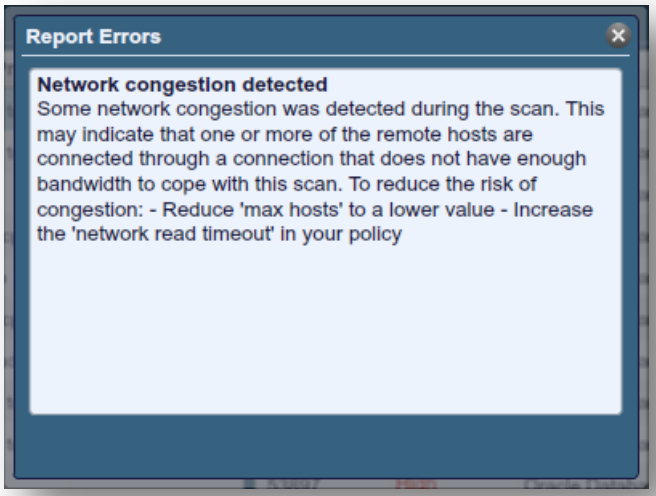
Wählen Sie zum Durchsuchen der Ergebnisse eines Scans einen Namen aus der Liste „**Reports**“ aus und klicken Sie auf „**Browse**“. Nun können Sie die unterschiedlichen Resultate anzeigen, indem Sie zu Sicherheitslücken oder Hosts

navigieren und dabei Ports und spezifische Sicherheitslückeninformationen anzeigen. Die Standardansicht zeigt eine Zusammenfassung nach Sicherheitslücken. Aufgelistet werden alle Sicherheitslücken, sortiert nach Schweregrad:

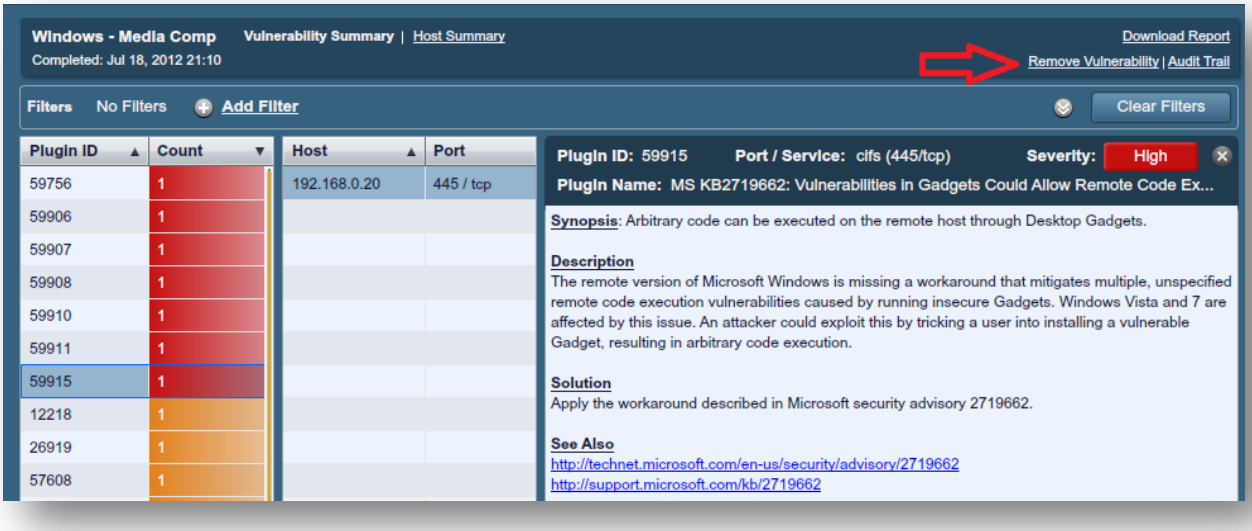

Nessus
admin | Help | About | Log out
Reports
Reports Mobile Scans Policies Users Configuration
Windows - Media Comp
Completed: Jul 18, 2012 21:10
Vulnerability Summary | Host Summary
Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter
Clear Filters
Plugin ID | Count | Severity | Name | Family
59756 | 1 | High | Winamp < 5.63 Multiple Vulnerabilities | Windows
59906 | 1 | High | MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Co | Windows : Microsoft Bulletins
59907 | 1 | High | MS12-044: Cumulative Security Update for Internet Explorer (2719177) | Windows : Microsoft Bulletins
59908 | 1 | High | MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Rem | Windows : Microsoft Bulletins
59910 | 1 | High | MS12-047: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevatior | Windows : Microsoft Bulletins
59911 | 1 | High | MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution | Windows : Microsoft Bulletins
59915 | 1 | High | MS KB2719662: Vulnerabilities in Gadgets Could Allow Remote Code Execution | Windows : Microsoft Bulletins
12218 | 1 | Medium | mDNS Detection | Service detection
26919 | 1 | Medium | Microsoft Windows SMB Guest Account Local User Access | Windows
57608 | 1 | Medium | SMB Signing Disabled | Misc.

Wenn während des Scans Fehler aufgetreten sind, erscheint neben der Datumsangabe „Completed“ (Abgeschlossen) ein entsprechender Hinweis. Wenn Sie den Fehlerhinweis anklicken, erhalten Sie weitere Informationen:

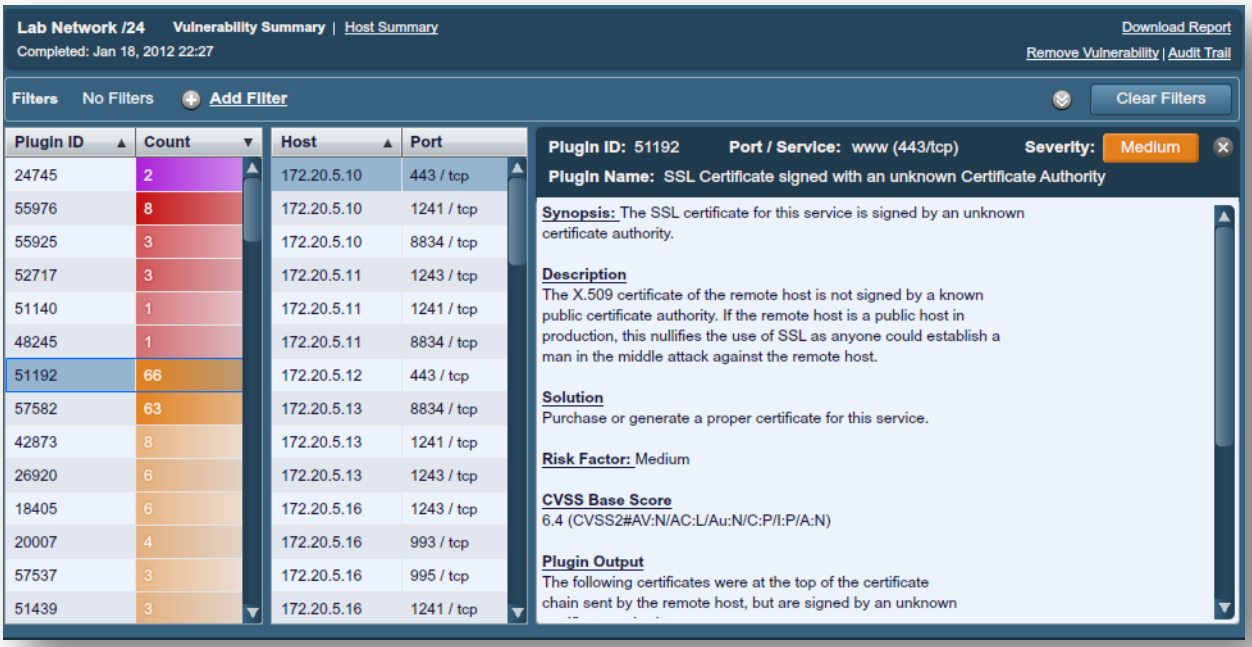

Reports
Reports Scans Policies Users
CIS XP Benchmark
Vulnerability Summary | Host Summary
Completed: Jan 20, 2012 12:52 (1 Error)
Filters No Filters Add Filter
Host | Vulnerabilities | Port/Prot | Vulnerabilities


Report Errors
Network congestion detected
Some network congestion was detected during the scan. This may indicate that one or more of the remote hosts are connected through a connection that does not have enough bandwidth to cope with this scan. To reduce the risk of congestion: - Reduce 'max hosts' to a lower value - Increase the 'network read timeout' in your policy

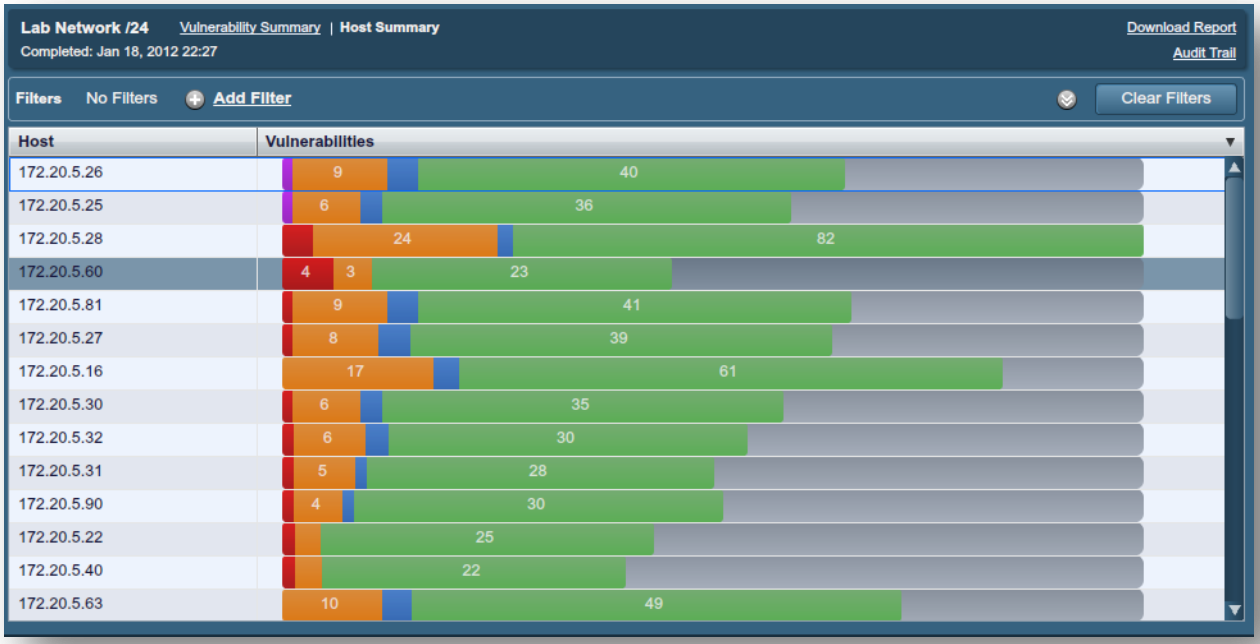
In der Ansicht „**Vulnerability Summary**“ („Übersicht zu Sicherheitslücken“) kann der Benutzer Sicherheitslücken gezielt aus dem Bericht entfernen. Bei Auswahl einer Sicherheitslücke werden weitere Informationen zu den betroffenen Hosts und Ports sowie technische Angaben zur jeweiligen Sicherheitslücke angezeigt. Über die Option „**Remove Vulnerability**“ („Sicherheitslücke entfernen“) kann die ausgewählte Sicherheitslücke entfernt werden:


Windows - Media Comp
Completed: Jul 18, 2012 21:10
Vulnerability Summary | Host Summary
Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter
Clear Filters
Plugin ID Count
59756 1
59906 1
59907 1
59908 1
59910 1
59911 1
59915 1
12218 1
26919 1
57608 1
Host Port
192.168.0.20 445 / tcp
Plugin ID: 59915 Port / Service: cifs (445/tcp) Severity: High
Plugin Name: MS KB2719662: Vulnerabilities in Gadgets Could Allow Remote Code Ex...
Synopsis: Arbitrary code can be executed on the remote host through Desktop Gadgets.
Description
The remote version of Microsoft Windows is missing a workaround that mitigates multiple, unspecified remote code execution vulnerabilities caused by running insecure Gadgets. Windows Vista and 7 are affected by this issue. An attacker could exploit this by tricking a user into installing a vulnerable Gadget, resulting in arbitrary code execution.
Solution
Apply the workaround described in Microsoft security advisory 2719662.
See Also
http://technet.microsoft.com/en-us/security/advisory/2719662
http://support.microsoft.com/kb/2719662

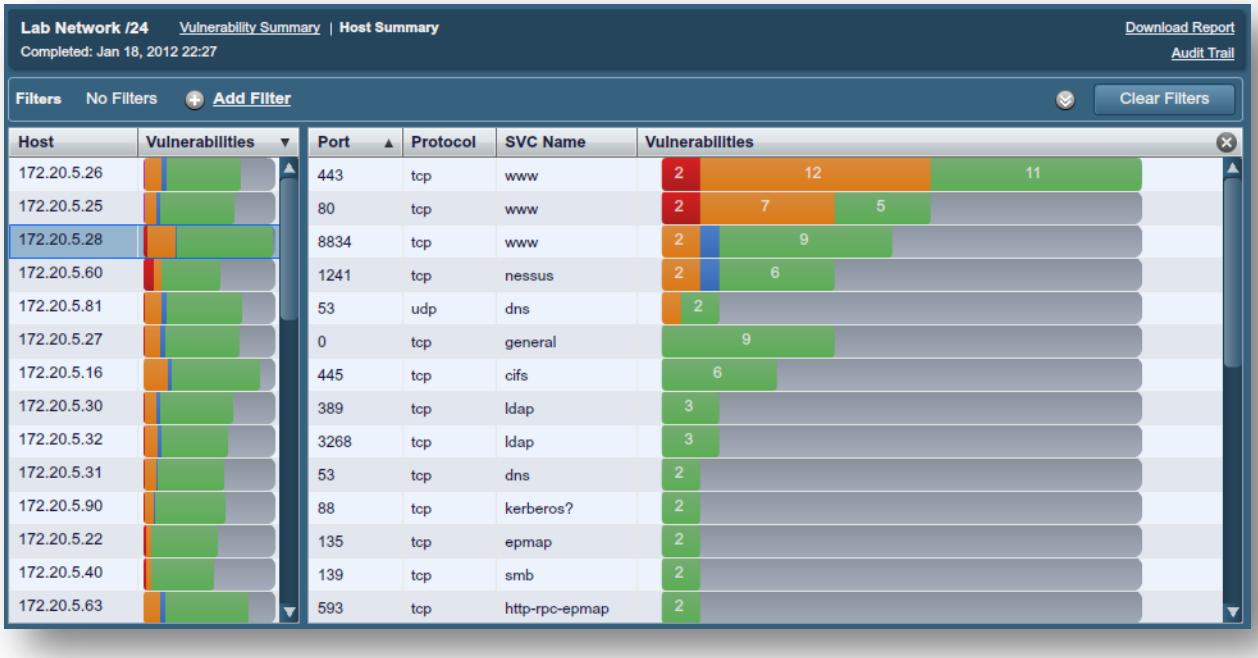
Bei der Navigation durch die Scanergebnisse werden auf der Benutzeroberfläche eine Liste der betroffenen Hosts und Ports sowie zusätzliche Informationen zur jeweiligen Sicherheitslücke angezeigt:


Lab Network /24 Vulnerability Summary | Host Summary
Completed: Jan 18, 2012 22:27
Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter
Clear Filters
Plugin ID Count
24745 2
55976 8
55925 3
52717 3
51140 1
48245 1
51192 66
57582 63
42873 8
26920 6
18405 6
20007 4
57537 3
51439 3
Host Port
172.20.5.10 443 / tcp
172.20.5.10 1241 / tcp
172.20.5.10 8834 / tcp
172.20.5.11 1243 / tcp
172.20.5.11 1241 / tcp
172.20.5.11 8834 / tcp
172.20.5.12 443 / tcp
172.20.5.13 8834 / tcp
172.20.5.13 1241 / tcp
172.20.5.13 1243 / tcp
172.20.5.16 1243 / tcp
172.20.5.16 993 / tcp
172.20.5.16 995 / tcp
172.20.5.16 1241 / tcp
Plugin ID: 51192 Port / Service: www (443/tcp) Severity: Medium
Plugin Name: SSL Certificate signed with an unknown Certificate Authority
Synopsis: The SSL certificate for this service is signed by an unknown certificate authority.
Description
The X.509 certificate of the remote host is not signed by a known public certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.
Solution
Purchase or generate a proper certificate for this service.
Risk Factor: Medium
CVSS Base Score
6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
Plugin Output
The following certificates were at the top of the certificate chain sent by the remote host, but are signed by an unknown

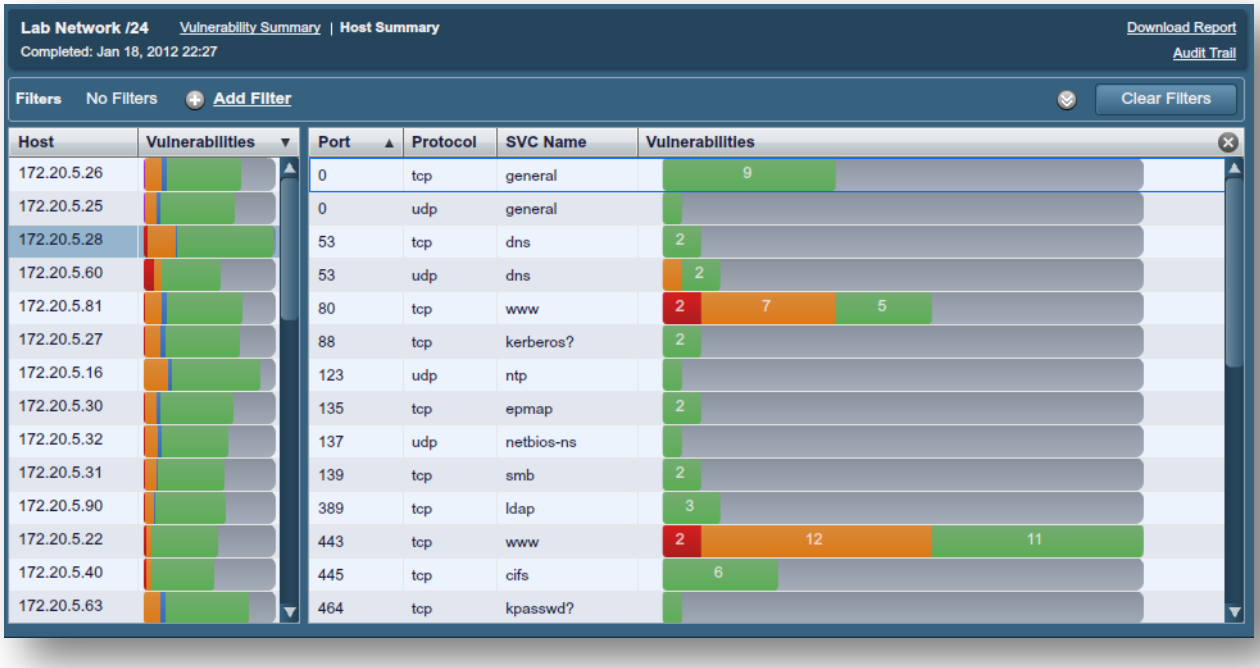
Um zwischen den Zusammenfassungen zu Sicherheitslücken und Hosts zu wechseln, können Sie oben auf dem Bildschirm neben dem Namen des Scans die gewünschte Ansicht auswählen:



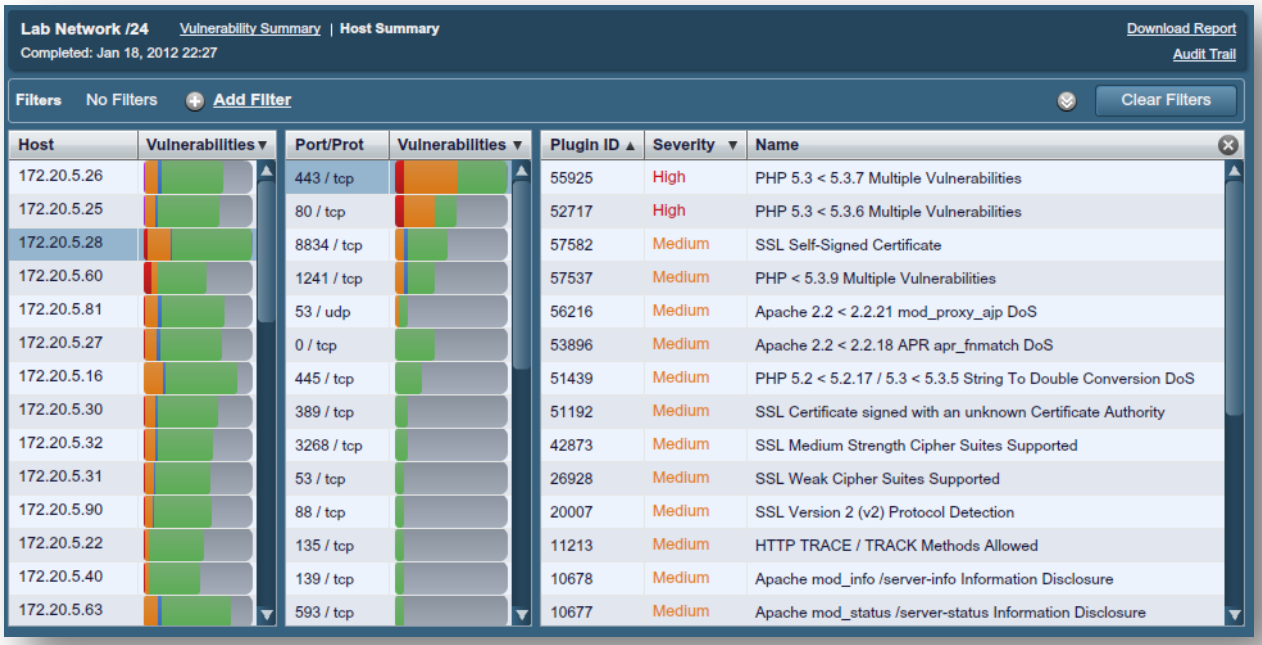
Bei Auswahl eines Hosts werden alle ihm zugeordneten gefundenen Sicherheitslücken nach Ports sortiert aufgelistet:



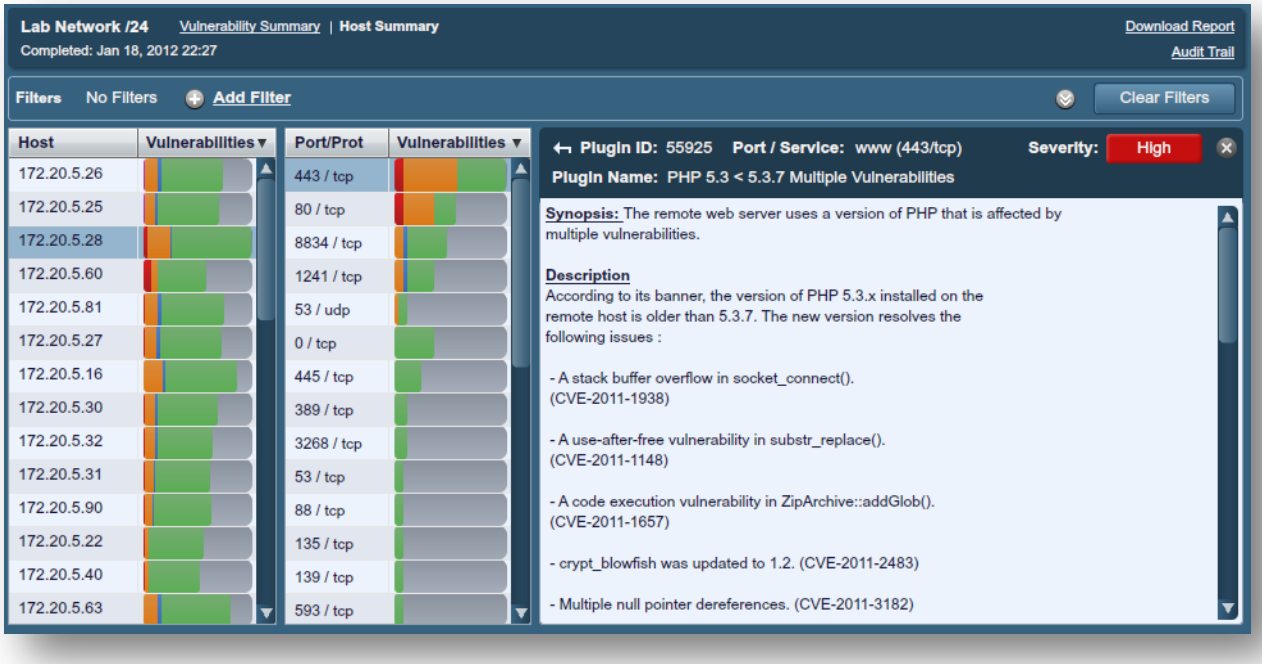
Im obigen Beispiel weist Host 172.20.5.60 insgesamt 30 Sicherheitslücken und 82 von Plugins generierte Hinweise auf. Für jeden Port werden das Protokoll, der Dienstname und eine farbige Darstellung der auf dem Port gefundenen Sicherheitslücken angezeigt. Durch Anklicken der Spaltenüberschriften können die Ergebnisse entsprechend dem Inhalt der betreffenden Spalte sortiert werden. Durch erneutes Anklicken wird die Sortierreihenfolge umgekehrt:



Die Auswahl eines Ports aus der Liste ruft eine Liste mit zugehörigen Sicherheitslücken sowie Angaben zur jeweiligen Plugin-ID und zum Schweregrad auf:



Wenn Sie auf eine Sicherheitslücke klicken, werden entsprechende Details angezeigt. Diese umfassen eine Zusammenfassung, Beschreibung, Lösung, Verweise auf Drittanbieter, den Risikofaktor, CVSS-Bewertungen, die Plugin-Ausgabe (sofern vorhanden) und Angaben bezüglich der Frage, ob ein öffentlicher Exploit verfügbar ist (z. B. ein öffentliches oder ein Exploit-Framework):



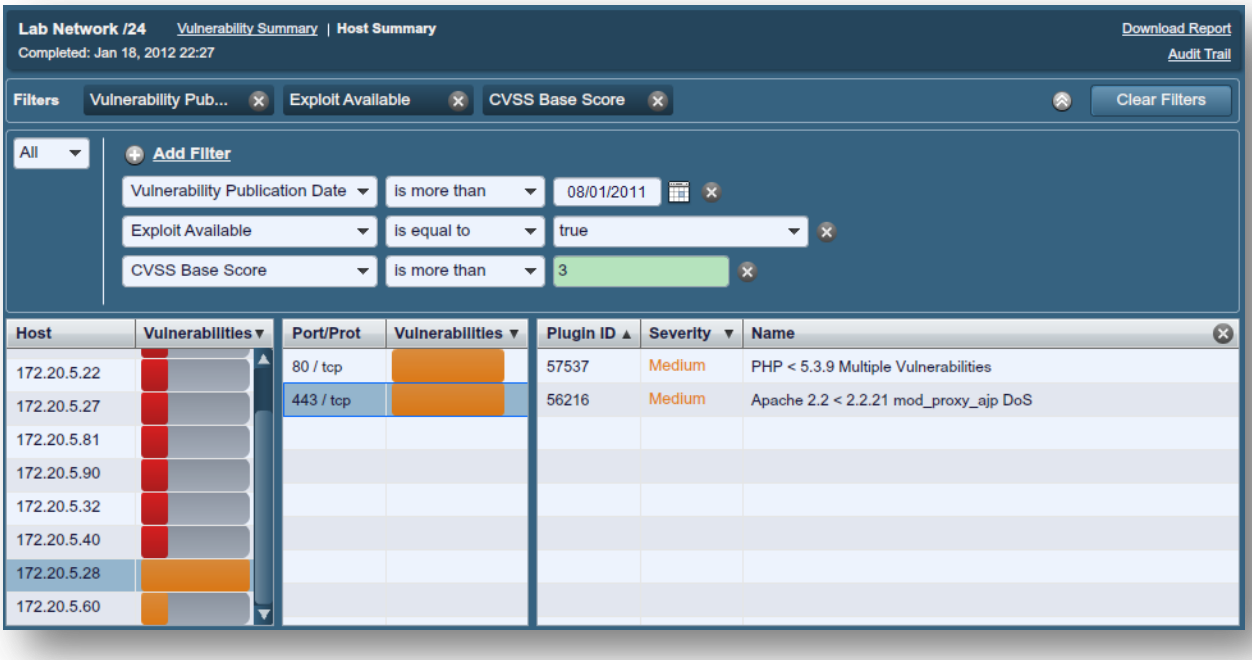
Das Fenster mit den Sicherheitslückendetails weist auf beiden Seiten einen Navigationspfeil auf, mit dem alle Sicherheitslücken nacheinander aufgerufen werden können:

Plugin ID: 57582 Port / Service: www (443/tcp) Severity: Medium
Plugin Name: SSL Self-Signed Certificate
Synopsis: The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
Description
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.
Solution
Purchase or generate a proper certificate for this service.
Risk Factor: Medium
CVSS Base Score
6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Berichtsfilter

Nessus bietet ein flexibles Filtersystem, mit dem die Anzeige bestimmter Berichtsresultate vereinfacht wird. Mithilfe von Filtern lassen sich Ergebnisse basierend auf jedem beliebigen Aspekt der gefundenen Sicherheitslücken anzeigen. Werden mehrere Filter verwendet, dann lassen sich detaillierte und angepasste Berichtsansichten erstellen.

Klicken Sie zur Erstellung eines Filters zunächst auf „**Add Filters**“ („Filter hinzufügen“) über den Suchergebnissen. Filter lassen sich aus der Berichtszusammenfassung oder den Übersichtsfenstern auf der Host- und der Portebene erstellen. Mehrere Filter können durch logische Bedingungen verknüpft werden, was eine komplexe Filterung gestattet. Ein Filter wird erstellt, indem das Plugin-Attribut, ein Filterargument und ein zu filternder Wert ausgewählt werden: Bei Auswahl mehrerer Filter sollten die Schlüsselwörter „Any“ bzw. „All“ entsprechend angegeben werden. Bei Auswahl von „All“ werden Ergebnisse angezeigt, die die Kriterien **aller** Filter erfüllen:



Wenn ein Filter festgelegt wurde, kann er durch Anklicken von ⊗ auf der rechten Seite bzw. der Filterschaltfläche entfernt werden. Durch Auswahl von „Clear Filters“ („Alle Filter löschen“) können alle Filter entfernt werden. Die Berichtsfilter unterstützen eine Vielzahl von Kriterien zur fein abgestuften Steuerung der Ergebnisse:

Option	Beschreibung
Plugin ID (Plugin-ID)	Filtert Ergebnisse, wenn die Plugin-ID einer bestimmten Zeichenfolge (z. B. 42111) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Description (Plugin-Beschreibung)	Filtert Ergebnisse, wenn die Plugin-Beschreibung eine bestimmte Zeichenfolge (z. B. „remote“) enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Name (Plugin-Name)	Filtert Ergebnisse, wenn der Plugin-Name einer bestimmten Zeichenfolge (z. B. „windows“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Family (Plugin-Familie)	Filtert Ergebnisse, wenn der Plugin-Name einer der angegebenen Nessus-Plugin-Familien entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“). Die möglichen Entsprechungen werden über ein Dropdownmenü bereitgestellt.
Plugin Output (Plugin-Ausgabe)	Filtert Ergebnisse, wenn die Plugin-Beschreibung einer bestimmten Zeichenfolge (z. B. „PHP“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Type (Plugin-Typ)	Filtert Ergebnisse, wenn der Plugin-Typ einem der folgenden beiden Plugin-Typen entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“): „local“ („lokal“), „remote“.
Solution (Lösung)	Filtert Ergebnisse, wenn die Plugin-Lösung eine bestimmte Zeichenfolge (z. B. „upgrade“) enthält („*contains*“) bzw. nicht enthält („*does not contain*“).

Synopsis (Zusammenfassung)	Filtert Ergebnisse, wenn die Plugin-Zusammenfassung eine bestimmte Zeichenfolge (z. B. „PHP“) enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Hostname	Filtert Ergebnisse, wenn der Host einer bestimmten Zeichenfolge (z. B. „192.168“ oder „lab“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Port	Filtert Ergebnisse basierend darauf, ob ein Port einer bestimmten Zeichenfolge (z. B. „80“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Protocol (Protokoll)	Filtert Ergebnisse, wenn ein Protokoll einer bestimmten Zeichenfolge (z. B. „http“) entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“).
CPE	Filtert Ergebnisse basierend darauf, ob die Common Platform Enumeration (CPE) einer bestimmten Zeichenfolge (z. B. „solaris“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVSS Base Score (CVSS-Basisbewertung)	Filtert Ergebnisse basierend darauf, ob die CVSS-Basisbewertung kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „5“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“). Mithilfe dieses Filters kann nach Risikostufe ausgewählt werden. Die Schweregradbewertungen sind von der zugehörigen CVSS-Bewertung abgeleitet. Dabei wird eine Punktzahl von 0 als „Information“, ein Wert von unter 4 als „niedrig“, von unter 7 als „moderat“, von unter 10 als „hoch“ und von 10 oder höher als „kritisch“ gewertet.
CVSS Temporal Score (CVSS-Temporärbewertung)	Filtert Ergebnisse basierend darauf, ob die CVSS-Temporärbewertung kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „3.3“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVSS Temporal Vector (CVSS-Temporärvektor)	Filtert Ergebnisse basierend darauf, ob der CVSS-Temporärvektor einer bestimmten Zeichenfolge (z. B. „E:F“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVSS Vector (CVSS-Vektor)	Filtert Ergebnisse basierend darauf, ob der CVSS-Vektor einer bestimmten Zeichenfolge (z. B. „AV:N“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Vulnerability Publication Date (Veröffentlichungsdatum der Sicherheitslücke)	Filtert Ergebnisse basierend darauf, ob das Veröffentlichungsdatum einer Sicherheitslücke zeitlich früher („*earlier than*“) oder später („*later than*“) als eine Zeichenfolge (z. B. „01/01/2012“) liegt, dem Wert der Zeichenfolge entspricht („*on*“) oder nicht entspricht („*not on*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“). Hinweis: Wenn Sie auf die Schaltfläche neben dem Datum klicken, wird ein Kalender angezeigt, in dem Sie das Datum auswählen können.

Patch Publication Date (Veröffentlichungsdatum des Patchs)	Filtert Ergebnisse basierend darauf, ob das Veröffentlichungsdatum des Patchs zu einer Sicherheitslücke kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „12/01/2011“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Publication Date (Veröffentlichungsdatum des Plugins)	Filtert Ergebnisse basierend darauf, ob das Veröffentlichungsdatum eines Nessus-Plugins kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „06/03/2011“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Modification Date (Änderungsdatum des Plugins)	Filtert Ergebnisse basierend darauf, ob das Änderungsdatum eines Nessus-Plugins kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „02/14/2010“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVE	Filtert Ergebnisse basierend darauf, ob ein CVE-Verweis einer bestimmten Zeichenfolge (z. B. „2011-0123“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Bugtraq ID (BugTraq-ID)	Filtert Ergebnisse basierend darauf, ob eine BugTraq-ID einer bestimmten Zeichenfolge (z. B. „51300“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CERT Advisory ID (CERT-Advisory-ID)	Filtert Ergebnisse basierend darauf, ob eine CERT-Advisory-ID (heißt mittlerweile „Technical Cyber Security Alert“) einer bestimmten Zeichenfolge (z. B. „TA12-010A“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
OSVDB ID	Filtert Ergebnisse basierend darauf, ob eine OSVDB-ID (Open Source Vulnerability Database) einer bestimmten Zeichenfolge (z. B. „78300“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Secunia ID	Filtert Ergebnisse basierend darauf, ob eine Secunia-ID einer bestimmten Zeichenfolge (z. B. „47650“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Exploit Database ID	Filtert Ergebnisse basierend darauf, ob eine EDB-ID (Exploit Database ID) einer bestimmten Zeichenfolge (z. B. „18380“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Metasploit Name (Metasploit-Name)	Filtert Ergebnisse basierend darauf, ob ein Metasploit-Name einer bestimmten Zeichenfolge (z. B. „xslt_password_reset“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Exploit Hub	Filtert Ergebnisse basierend darauf, ob ein ExploitHub-Exploit wahr („*true*“) oder falsch („*false*“) ist.
IAVA	Filtert Ergebnisse basierend darauf, ob eine IAVA-Referenz einer bestimmten Zeichenfolge (z. B. „2012-A-0008“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).

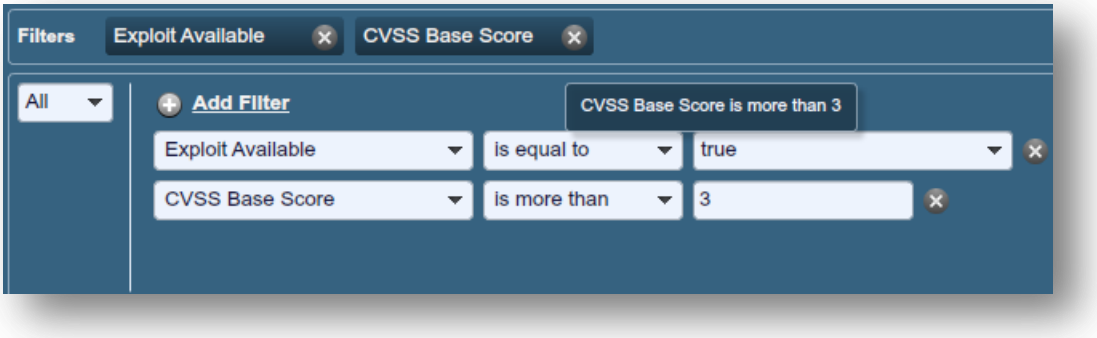
See Also (Siehe auch)	Filtert Ergebnisse basierend darauf, ob ein „See also“-Verweis (Querverweis) eines Nessus-Plugins einer bestimmten Zeichenfolge (z. B. „seclists.org“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Exploits Available (Exploits verfügbar)	Filtert Ergebnisse basierend darauf, ob für die betreffende Sicherheitslücke ein Exploit existiert.
Exploitability Ease	Filtert Ergebnisse basierend darauf, ob die „Exploitability Ease“ (also die Frage, wie einfach die Sicherheitslücke genutzt werden kann) einem der folgenden Werte entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“): „*Exploits are available*“ („Exploits vorhanden“), „*No exploit is required*“ („Keine Exploits benötigt“) oder „*No known exploits are available*“ („Keine bekannten Exploits vorhanden“).
Metasploit Exploit Framework	Filtert Ergebnisse basierend darauf, ob eine Sicherheitslücke im Metasploit Exploit Framework „true“ oder „false" entspricht („*is equal to*“).

Bei der Verwendung eines Filters kann der String bzw. der Zahlenwert auch kommagetrennt sein, um nach mehreren Strings zu filtern. Um beispielsweise nur Ergebnisse anzuzeigen, die sich auf Webserver beziehen, könnten Sie einen Filter „Ports“ erstellen, als Filterbedingung „is equal to“ und als Eingabewert „80,443,8000,8080“ festlegen. Auf diese Weise werden Ihnen nur Ergebnisse zu diesen vier Ports angezeigt.

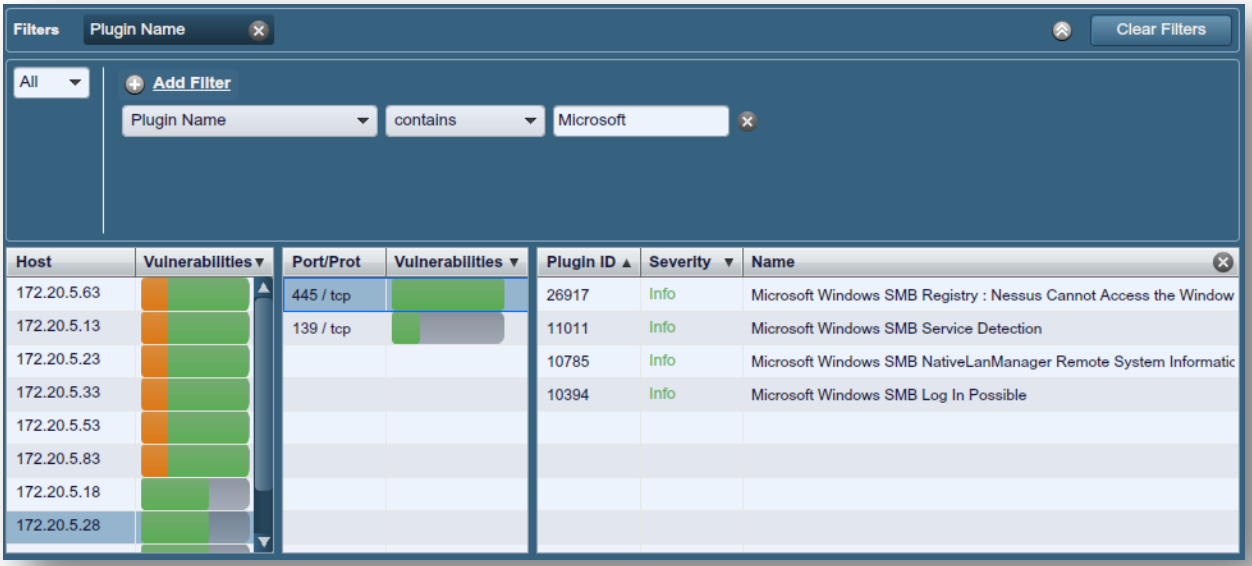
Bei Filterkriterien wird die Groß-/Kleinschreibung **nicht** unterschieden.

Wenn eine Filteroption nicht verfügbar ist, bedeutet dies, dass der Bericht keine den Kriterien entsprechenden Inhalte hat. Ist beispielsweise „Microsoft Bulletin“ nicht in der Filter-Dropdownliste vorhanden, dann wurden keine Sicherheitslücken gefunden, die auf ein Microsoft-Bulletin verweisen.

Nach ihrer Erstellung erscheinen Filter in der Liste über dem Filtereingabebereich. Um aktive Filterdetails anzuzeigen, setzen Sie den Mauszeiger auf den Filternamen:

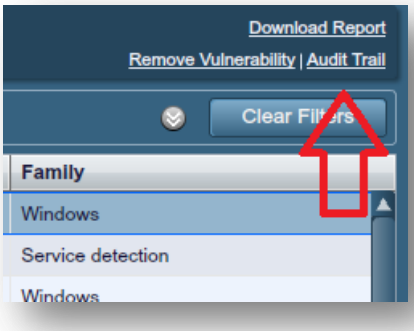


Sobald ein Filter erstellt ist, werden die Scanergebnisse entsprechend den neuen Filterkriterien aktualisiert. Im nachfolgenden Beispiel werden durch Erstellung eines Filters, der nur Ergebnisse mit dem String „Microsoft“ im Plugin-Namen anzeigt, die meisten Ergebnisse entfernt:

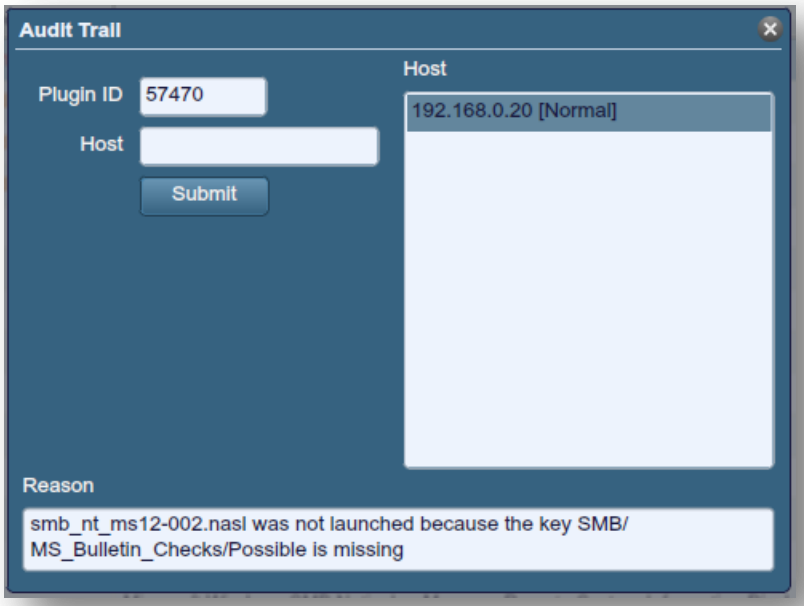


Wenn die Ergebnisse so gefiltert wurden, dass die von Ihnen gewünschten Daten angezeigt werden, klicken Sie auf „**Download Report**“ („Bericht herunterladen“), um nur die gefilterten Ergebnisse zu exportieren. Benötigen Sie einen Bericht mit allen Ergebnissen, dann verwenden Sie die Downloadschaltfläche auf der Hauptseite „**Reports**“.

Die Nessus-Scanergebnisse bieten Ihnen einen schnellen Überblick über Plugins, von denen Probleme auf dem Host gefunden wurden. Manchmal wollen Sie allerdings wissen, warum ein Plugin keine Ergebnisse zurückgegeben hat. Hierfür ist die Funktion „Audit Trail“ gedacht. Klicken Sie zunächst auf das Symbol „Audit Trail“ oben rechts auf dem Bildschirm.



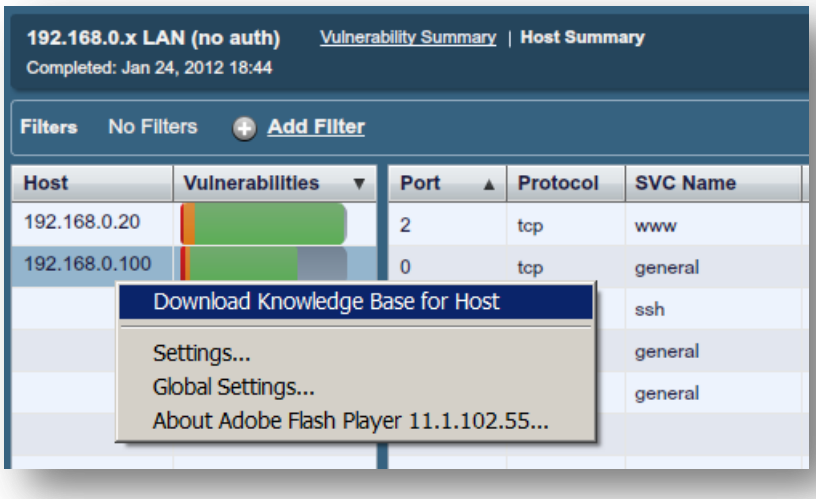
Dadurch wird die Seite „Audit Trail“ aufgerufen. Geben Sie nun die ID des Plugins ein, über das Sie mehr erfahren möchten. Klicken Sie auf „Submit“ („Absenden“). Nun werden ein oder mehrere Hosts angezeigt, die Ihrer Abfrage entsprechen. Optional können Sie eine Host-IP-Adresse bei der ersten Abfrage angeben, um die Ergebnisse auf das gewünschte Ziel zu beschränken. Wenn der oder die gefundenen Hosts angezeigt werden, klicken Sie auf die gewünschte Information, um zu erfahren, warum ein Plugin kein Ergebnis gefunden hat:



Da ein Audit-Trail sehr ressourcenintensiv ist, stehen unter bestimmten Umständen nur eingeschränkte Audit-Trails zur Verfügung. Wird nur ein Host gescannt, dann erfolgt der Audit-Trail vollständig. Bei zwei bis 512 gescannten Hosts sind für einen vollständigen Audit-Trail mindestens zwei CPUs und 2 GB Arbeitsspeicher erforderlich. Bei mehr als 512 Hosts wird immer nur ein eingeschränkter Audit-Trail ausgeführt.

In Nessus 5 wird bei jedem Scan eine Wissensdatenbank (Knowledge Base, KB) gespeichert. Es handelt sich hierbei um eine ASCII-Textdatei mit Protokollangaben zum durchgeführten Scan und den gefundenen Ergebnissen. Eine KB ist häufig nützlich, wenn Sie Unterstützung von Tenable benötigen: Mit ihrer Hilfe kann der Supportmitarbeiter nachvollziehen, was genau Nessus tat und welche Daten gefunden wurden.

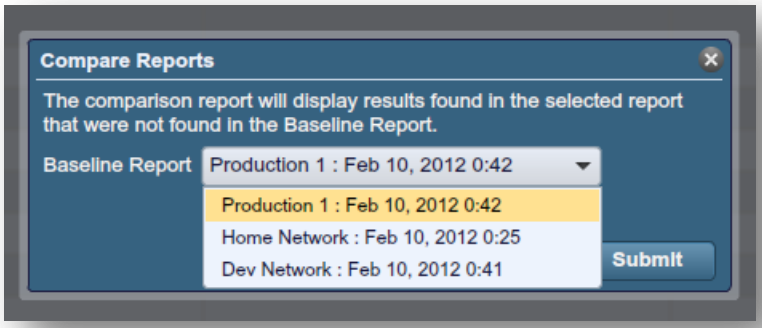
Klicken Sie zum Herunterladen einer KB mit der rechten Maustaste auf einen Hostnamen und wählen Sie „Download Knowledge Base for Host“ („Wissensdatenbank für Host herunterladen“) aus:



Compare (Vergleichen)

In Nessus können Sie zwei Scanberichte miteinander vergleichen, um Unterschiede anzuzeigen. Durch die Möglichkeit, Unterschiede zwischen Scans anzuzeigen, lässt sich feststellen, wie sich ein gegebenes System oder Netzwerk im Laufe der Zeit verändert hat. Dies erleichtert Complianceanalysen, denn Sie können so erkennen, welche Sicherheitslücken geschlossen wurden, ob Systeme bei Feststellung neuer Sicherheitslücken entsprechend gepatcht wurden oder dass zwei Scans möglicherweise nicht die gleichen Hosts verarbeiten.

Wählen Sie zum Vergleich von Berichten zunächst einen Scan aus der Liste „**Reports**“ (Berichte) aus und klicken Sie dann in der Menüleiste rechts auf „**Compare**“ (Vergleichen). Das resultierende Dialogmenü enthält eine Dropdownliste mit anderen Berichten, die verglichen werden können. Wählen Sie einen Bericht aus und klicken Sie auf „**Submit**“ (Absenden):


Compare Reports
The comparison report will display results found in the selected report that were not found in the Baseline Report.
Baseline Report
Production 1 : Feb 10, 2012 0:42
Production 1 : Feb 10, 2012 0:42
Home Network : Feb 10, 2012 0:25
Dev Network : Feb 10, 2012 0:41
Submit

Nessus vergleicht den ersten ausgewählten Bericht mit dem zweiten und generiert eine Liste mit Ergebnissen, die sich seit dem ersten Bericht geändert haben. Die Vergleichsfunktion zeigt nicht die Unterschiede zwischen zwei beliebigen Berichten, sondern stellt die Änderungen dar, die seit dem ersten Bericht (der Baseline) stattgefunden haben. An diesen Ergebnissen lässt sich also ablesen, welche Sicherheitslücken zwischen den beiden Scans gefunden bzw. behoben wurden. Im obigen Beispiel ist „LAN Scan One“ ein Scan des gesamten Subnetzes 192.168.0.0/24 und „LAN Scan Two“ ein Scan dreier ausgewählter Hosts im selben Subnetz. Die Funktion „Compare“ zeigt die Unterschiede an, indem Hosts, die in „LAN Scan Two“ nicht gescannt wurden, hervorgehoben werden:

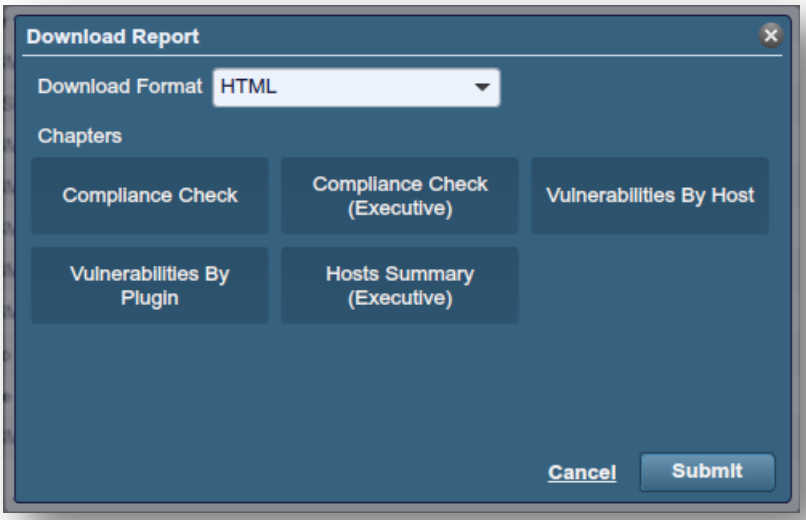
Plugin ID	Count	Severity	Name	Family
51192	2	Medium	SSL Certificate Cannot Be Trusted	General
57608	1	Medium	SMB Signing Not Required	Misc.
57582	1	Medium	SSL Self-Signed Certificate	General
14272	18	Info	netstat portscanner (SSH)	Port scanners
22964	9	Info	Service Detection	Service detection
10736	8	Info	DCE Services Enumeration	Windows
56984	2	Info	SSL / TLS Versions Supported	General
54615	2	Info	Device Type	General
45590	2	Info	Common Platform Enumeration (CPE)	General
21643	2	Info	SSL Cipher Suites Supported	General

Die Funktion „Compare“ steht nur ProfessionalFeed-Benutzern zur Verfügung.

Upload und Download

Scanergebnisse können aus einem Nessus-Scanner exportiert und in einen anderen importiert werden. Die Funktionen „**Upload**“ und „**Download**“ erleichtern Scanmanagement, Berichtsvergleich, Sicherung von Berichten und die Kommunikation zwischen Gruppen und Organisationen innerhalb eines Unternehmens.

Wählen Sie den zu exportierenden Scan aus der Liste „**Reports**“ aus und klicken Sie auf „**Download**“. Nun wird ein Dialogfeld zum Herunterladen von Berichten angezeigt, in dem Sie aufgefordert werden, das gewünschte Format sowie die einzuschließenden (in „Kapitel“ unterteilten) Daten anzugeben. Wenn Sie auf ein Kapitel klicken, wird dieses entsprechend markiert und in den Bericht eingebunden:



Nur mit Nessus 5 durchgeführte Compliancescans können mit Compliancekapiteln im PDF- oder HTML-Format exportiert werden. Ein Export importierter Scans aus früheren Nessus-Versionen ist in dieser Form nicht möglich.

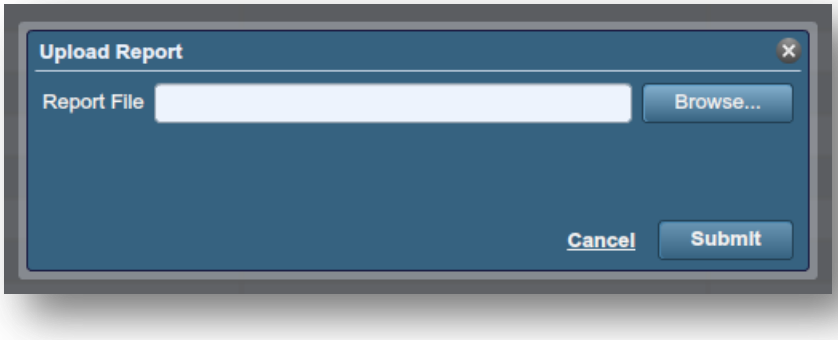
Berichte können in verschiedenen Formaten heruntergeladen werden. Beachten Sie, dass eine Kapitelauswahl bei einigen Formaten nicht möglich ist, da diese alle Angaben enthalten.

Option	Beschreibung
`.nessus`	Dieses XML-basierte Format ist der De-facto-Standard in Nessus 4.2 und höher. Es verwendet einen erweiterten Satz XML-Tags, um das Extrahieren und Analysieren von Informationen granularer zu gestalten. Dieser Bericht gestattet keine Kapitelauswahl.
`.nessus` **(v1)**	Ein XML-basiertes Format, das in Nessus 3.2 bis 4.0.2 verwendet wurde. Es ist kompatibel mit Nessus 4.x und Security Center 3 und gestattet keine Kapitelauswahl.
HTML	Ein in Standard-HTML generierter Bericht, der eine Kapitelauswahl gestattet. Der Bericht wird auf einer neuen Registerkarte in Ihrem Browser geöffnet.
PDF	Ein im PDF-Format generierter Bericht, der eine Kapitelauswahl gestattet. Je nach Größe des Berichts kann die Generierung der PDF-Datei mehrere Minuten in Anspruch nehmen.

	Oracle Java (vormals Sun Microsystems Java) ist für die Generierung von PDF-Berichten erforderlich.
CSV	Ein Export mit kommagetrennten Werten (CSV) kann zum Import in eine Reihe externer Programme wie Datenbanken, Tabellenkalkulationsprogramme und mehr verwendet werden. Der Bericht lässt keine Kapitelauswahl zu.
NBE export (NBE-Export)	Exportdatei mit Trennzeichen, die in viele externe Programme importiert werden kann. Als Trennzeichen kommt der Längsstrich („|“) zum Einsatz. Dieser Bericht gestattet keine Kapitelauswahl.

Nach Auswahl der Formate **`.nessus`**, NBE oder PDF wird das Standarddialogfeld „Datei speichern“ Ihres Browsers angezeigt, in dem Sie die Scanergebnisse an einem Speicherort Ihrer Wahl speichern können. HTML-Berichte werden in Ihrem Browser angezeigt und können über die Browserfunktion „Datei > Speichern” gespeichert werden.

Klicken Sie zum Importieren eines Scans im Bildschirm „**Reports**“ oben links auf „**Upload Reports**“ („Berichte hochladen“):



Klicken Sie auf die Schaltfläche „**Browse…**“ („Durchsuchen“), wählen Sie die **`.nessus`**-Scandatei aus, die Sie importieren möchten, und klicken Sie auf „**Submit**“. Nessus analysiert die Daten und macht sie über die Oberfläche „**Reports**“ verfügbar.

Das .nessus-Dateiformat

Nessus verwendet zum Exportieren und Importieren ein bestimmtes Dateiformat: das **`.nessus`**-Format. Dieses Format bietet die folgenden Vorteile:

- Es ist XML-basiert, d. h. es bietet Aufwärts- und Abwärtskompatibilität und ist einfach zu implementieren.
- Es ist autark, d. h. die Liste der Ziele, die vom Benutzer definierten Richtlinien und die Scanergebnisse selbst sind in einer einzigen **`.nessus`**-Datei enthalten.
- Es ist sicher, denn Kennwörter werden nicht in der Datei gespeichert. Stattdessen wird ein Verweis auf ein Kennwort an einem sicheren Speicherort auf dem lokalen Host abgelegt.

Der Vorgang zur Erstellung einer **`.nessus`**-Datei mit den Zielen, Richtlinien und Scanergebnissen beginnt mit der Einrichtung und Speicherung der Richtlinie. Danach wird die Liste mit den Zieladressen generiert und abschließend ein Scan ausgeführt. Nach Abschluss des Scans können alle Daten in einer **`.nessus`**-Datei gespeichert werden. Hierzu wird die Option „**Download**“ auf der Registerkarte „**Reports**“ verwendet. Weitere Informationen zu **`.nessus`**-Dateien entnehmen Sie dem Dokument „Das Nessus V2-Dateiformat“.

Delete (Löschen)

Wenn Sie die Scanergebnisse nicht mehr benötigen und sie löschen möchten, wählen Sie den betreffenden Scan aus der Liste „Reports“ aus und klicken auf „**Delete**“. Auf diese Weise wird der Scan aus der Benutzeroberfläche gelöscht. **Dieser Vorgang kann nicht rückgängig gemacht werden!** Wenn Sie die Scanergebnisse vor dem Löschen exportieren möchten, verwenden Sie die Funktion „**Download**“.

Mobil

Nessus 5 ist in der Lage, Active Directory Service Interfaces und Apple Profile Manager zu scannen, was Scans von Beständen und Sicherheitslücken auf sowohl iOS-basierenden Geräten von Apple als auch Android-Geräten ermöglicht. Nessus lässt sich auf Authentifizierung auf diesen Servern sowie auf die Abfrage nach Mobilgeräteinformationen und Meldung eventueller Probleme mit diesen Geräten konfigurieren. Dies kann über eine übliche Scanrichtlinie oder im Register „**Mobile**“ erfolgen.

Zum Scannen auf Mobilgeräten muss Nessus mit Authentifizierungsangaben für den Verwaltungsserver und/oder die passenden Mobil-Plugins konfiguriert werden. Da Nessus Authentifizierungen direkt auf den Verwaltungsservern durchführt, muss zum Scannen spezifischer Hosts keine Scanrichtlinie konfiguriert sein.

Im Register „Mobile“ können der Apple Profile Manager und die ADSI-Informationen konfiguriert werden. Sobald die Details hinzugefügt und abgesendet wurden, scannt Nessus diese Server umgehend zum Abruf der Mobilgeräteinformationen. Durch erneutes Klicken auf dieses Register beginnt der Scan erneut, um aktuelle Informationen abzurufen.

Reports
Mobile
Scans
Policies
Users
Configuration
Nessus has the ability to monitor the patch level of the mobile devices used on your network by leveraging and combining data from multiple sources. You need at least one source of data to get results.
Active Sync
Nessus can use ActiveSync to gather information about all the mobile devices that used this protocol to fetch their email (via Exchange). If you have an Exchange deployment, please enter the following information below:
Profile Manager
Nessus can use Apple's Profile Manager to gather information about the iOS devices managed in your company. If you do have a Profile Manager deployment, please enter the information below (note that it is recommended that Nessus sends an 'update' request to every device and wait for their answer to get the newest data about them):
Apple Profile Manager Information
Server
Port
443
Username
Password
SSL
Force Device Updates
Device Update Timeout
5
minutes
ADSI Information
Domain Controller
Domain
Domain Username
Domain Password

Zum Start eines einfachen Mobilgerätescans werden lediglich die Angaben zum Active Directory oder dem MDM-Server benötigt. Nach Eingabe dieser Informationen wird der Scan gestartet und die Ergebnisse werden im Register „**Reports**“ (Berichte) angezeigt.

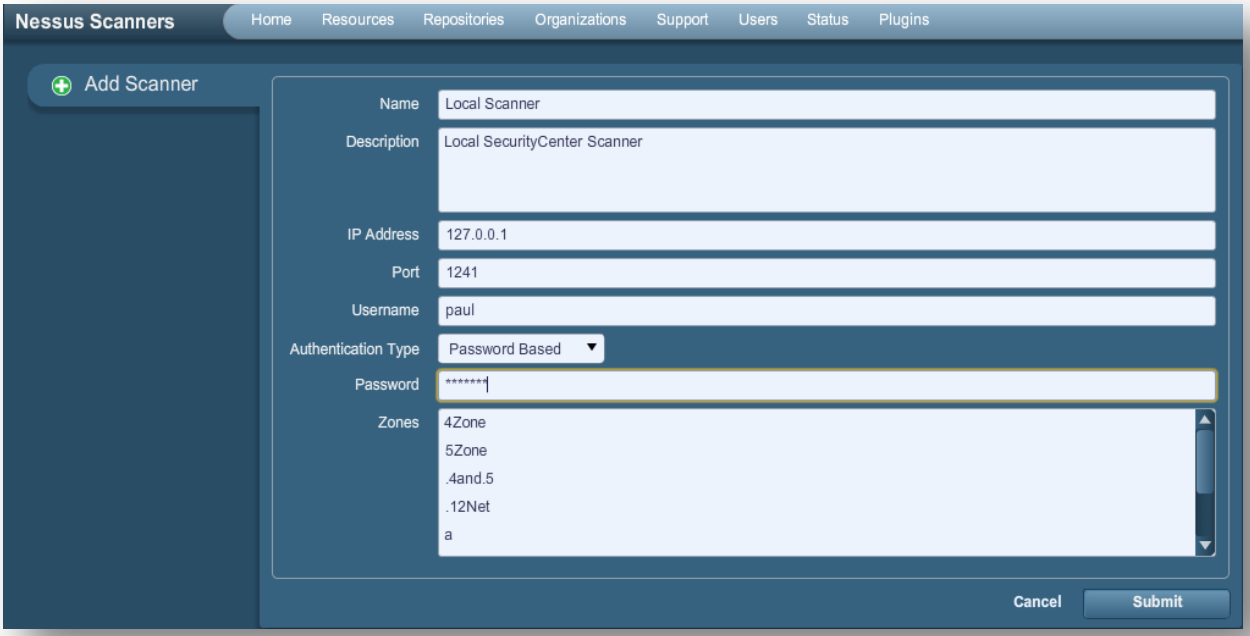
SecurityCenter

SecurityCenter 4.0 bis 4.2 für die Kooperation mit Nessus konfigurieren

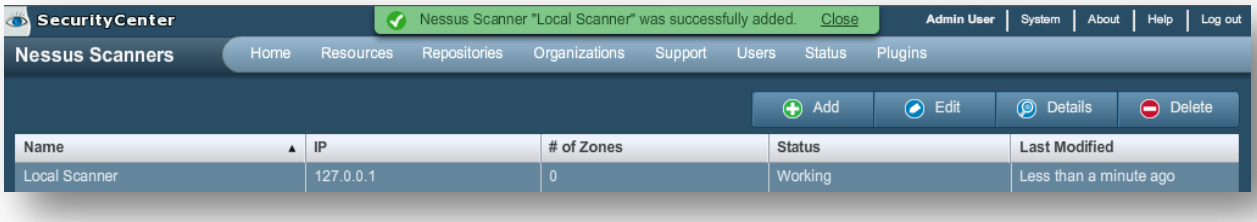
Ein Nessus-Server kann über die SecurityCenter-Verwaltungsoberfläche hinzugefügt werden. Mithilfe dieser Oberfläche lässt sich SecurityCenter so konfigurieren, dass von hier aus auf praktisch jeden Nessus-Scanner zugegriffen und dieser gesteuert werden kann. Klicken Sie auf die Registerkarte „Resources“ („Ressourcen“) und dann auf „**Nessus Scanners**“. Klicken Sie auf „**Add**“ („Hinzufügen“), um das Dialogfeld „Add Scanner“ („Scanner hinzufügen“) zu öffnen. Angegeben werden müssen die IP-Adresse des Nessus-Scanners, der Nessus-Port (Standard: 1241), der Anmeldename des

Administrators, der Authentifizierungstyp und das (bei der Konfiguration von Nessus erstellte) Kennwort. Die Kennwortfelder sind nicht verfügbar, wenn die Authentifizierung via SSL-Zertifikat (Option „SSL Certificate“) ausgewählt wird. Außerdem können unter „Zones“ Zonen festgelegt werden, denen der Nessus-Scanner zugeordnet werden kann.

Nachfolgend gezeigt ist eine Bildschirmabbildung der SecurityCenter-Seite „Add Scanner“:



Nach dem erfolgreichen Hinzufügen des Scanners wird die folgende Seite angezeigt:

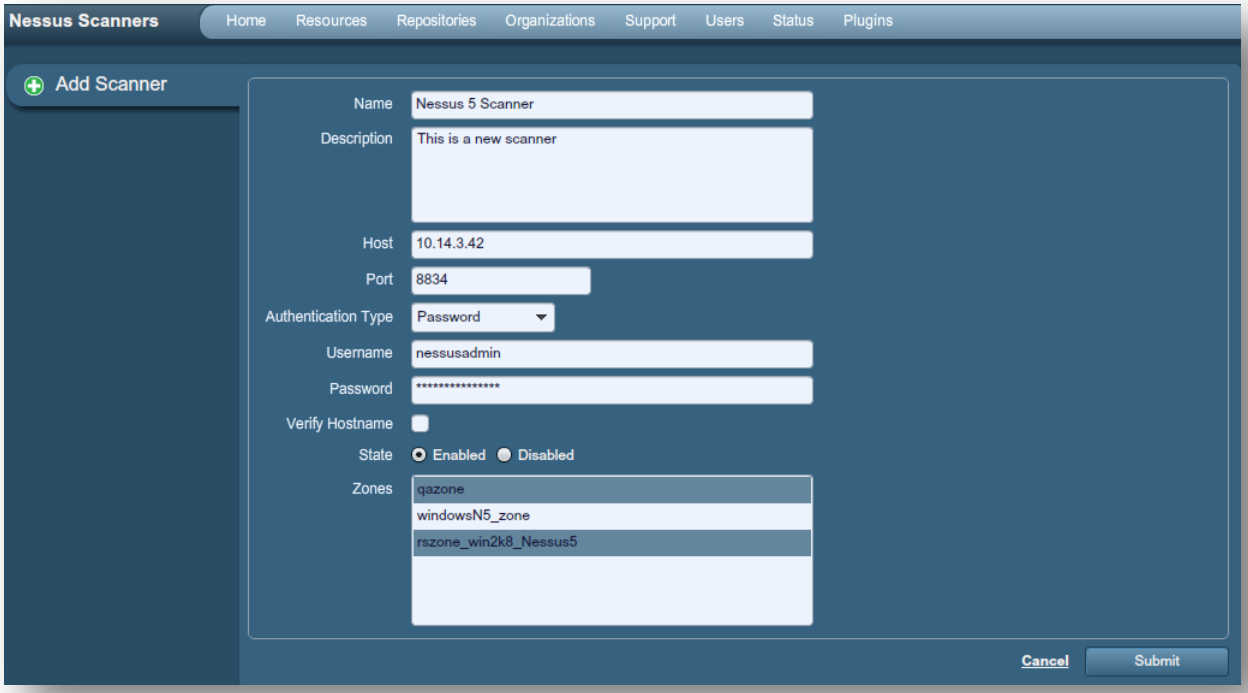


Weitere Informationen finden Sie im „SecurityCenter-Administrationshandbuch“.

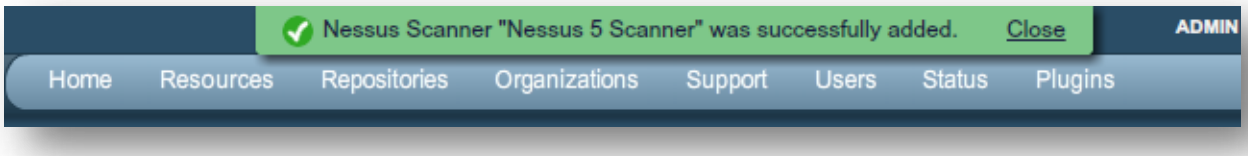
SecurityCenter 4.4 für die Kooperation mit Nessus konfigurieren

Mithilfe der SecurityCenter-Verwaltungsoberfläche können Zugriff und Steuerung beliebiger Nessus-Scanner mit der Versionsnummer 4.2.x oder höher konfiguriert werden. Klicken Sie auf die Registerkarte „**Resources**“ („Ressourcen“) und dann auf „**Nessus Scanners**“. Klicken Sie auf „**Add**“ („Hinzufügen“), um das Dialogfeld „**Add Scanner**“ („Scanner hinzufügen“) zu öffnen. Angegeben werden müssen die IP-Adresse oder der Hostname des Nessus-Scanners, der Nessus-Port (Standard: 8834), der bei der Konfiguration von Nessus erstellte Authentifizierungstyp sowie der Anmeldename des Administrators und das zugehörige Kennwort oder die erforderlichen Zertifikatsinformationen. Die Kennwortfelder sind nicht verfügbar, wenn die Authentifizierung via SSL-Zertifikat (Option „SSL Certificate“) ausgewählt wird. Die Funktion zur Überprüfung des Hostnamens ermöglicht die Verifizierung des CN (Common Name) im SSL-Zertifikat, das vom Nessus-Server übermittelt wurde. Der Status des Nessus-Scanners kann nach Bedarf auf „Enabled“ („Aktiviert“) oder „Disabled“ („Deaktiviert“) festgelegt werden. Die Standardeinstellung ist „Enabled“. Außerdem können Zonen ausgewählt werden, denen der Nessus-Scanner zugeordnet werden kann.

Nachfolgend gezeigt ist eine Bildschirmabbildung der Seite „**Add Scanner**“ aus SecurityCenter 4.4:



Nach dem erfolgreichen Hinzufügen des Scanners wird das folgende Banner angezeigt:



Weitere Informationen zur Integration von Nessus und SecurityCenter finden Sie im „SecurityCenter-Administrationshandbuch“.

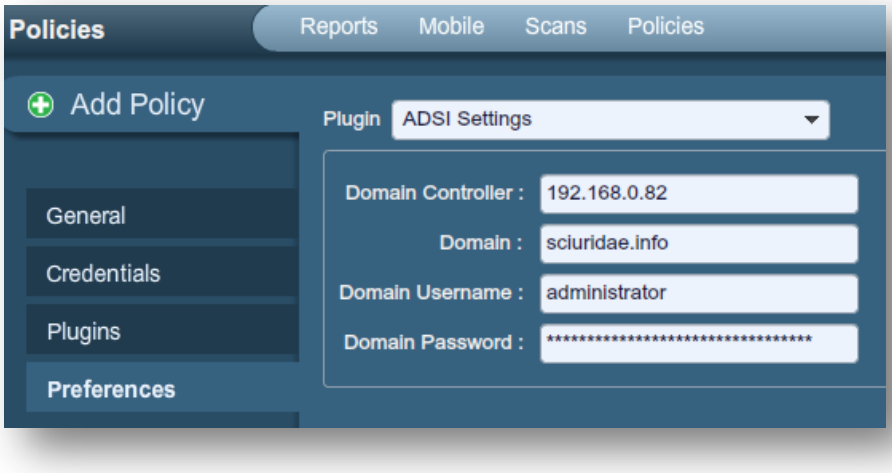
Hostbasierte Firewalls
Wenn Ihr Nessus-Server mit einer Personal Firewall wie beispielsweise Zone Alarm, Sygate, BlackICE, der Windows XP Firewall oder einer anderen Firewallsoftware konfiguriert ist, müssen Verbindungsanfragen von der IP-Adresse von SecurityCenter zugelassen werden.

Standardmäßig wird Port 8834 verwendet. Auf Systemen unter Microsoft XP Service Pack 2 und höher erhält der Benutzer nach Klick auf „**Sicherheitscenter**“ in der „**Systemsteuerung**“ die Möglichkeit, die Einstellungen der Windows-Firewall zu verwalten. Um Port 8834 zu öffnen, wählen Sie die Registerkarte „**Exceptions**“ (Ausnahmen) aus und fügen Sie der Liste Port 8834 hinzu.

Verwendet SecurityCenter das veraltete NTP-Protokoll über Port 1241, dann muss bei den obigen Befehlen 1241 anstelle von 8834 verwendet werden.

Details zu Scaneinstellungen

Die Registerkarte „**Preferences**“ („Voreinstellungen“) enthält knapp 40 Dropdownmenüs für eine fein abgestufte Steuerung der Scaneinstellungen. Nehmen Sie sich etwas Zeit, um die einzelnen Menüs kennen zu lernen und zu konfigurieren. Hierdurch erhalten Sie nicht nur mehr Flexibilität, sondern können auch im Vergleich zu Standardrichtlinien erheblich genauere Scanergebnisse erzielen Im nächsten Abschnitt sind die einzelnen Optionen der Registerkarte „**Preferences**“ ausführlich beschrieben. Beachten Sie, dass die Liste der Konfigurationsoptionen dynamisch ist, d. h. sie hängt vom Plugin-Feed, von den Auditrichtlinien und weiteren Funktionen ab, auf die der verbundene Nessus-Scanner zugreifen kann. Bei einem Scanner mit einem ProfessionalFeed stehen unter Umständen mehr fortgeschrittene Konfigurationsoptionen zur Verfügung als bei einem Scanner, für den der HomeFeed konfiguriert wurde. Außerdem kann sich diese Liste ändern, wenn Plugins hinzugefügt oder geändert werden.

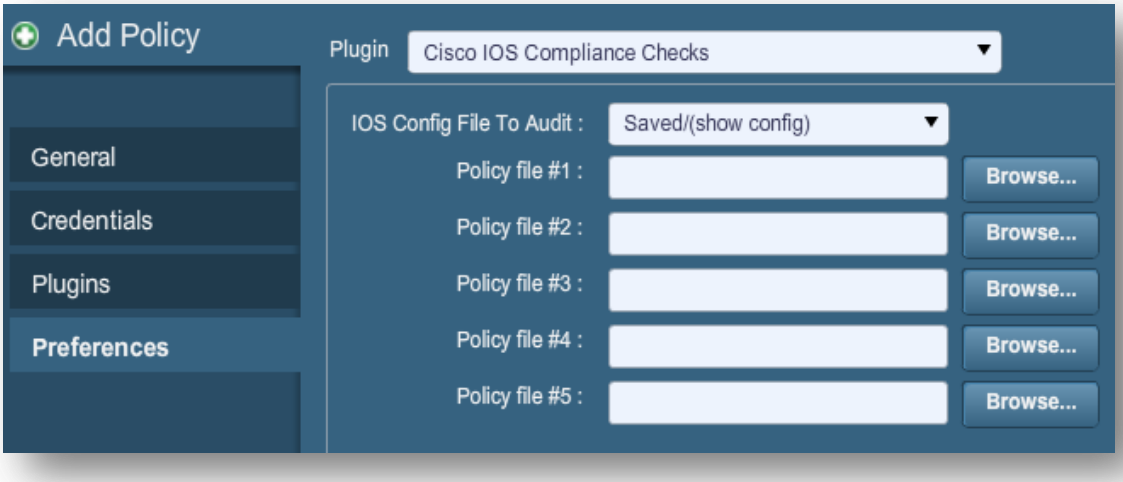


Mit den „**ADSI Settings**“ (ADSI-Einstellungen) kann Nessus den ActiveSync-Server abfragen, um festzustellen, ob Android- oder iOS-basierte Geräte angeschlossen sind. Nessus führt mithilfe der Anmeldedaten und Serverinformationen eine Authentifizierung auf dem Domänen-Controller (nicht dem Exchange-Server) durch, um die Geräteinformationen direkt abzufragen. Für diese Funktion müssen keine Ports in der Scanrichtlinie angegeben werden. Die Einstellungen werden für Scans von Mobilgeräten benötigt.

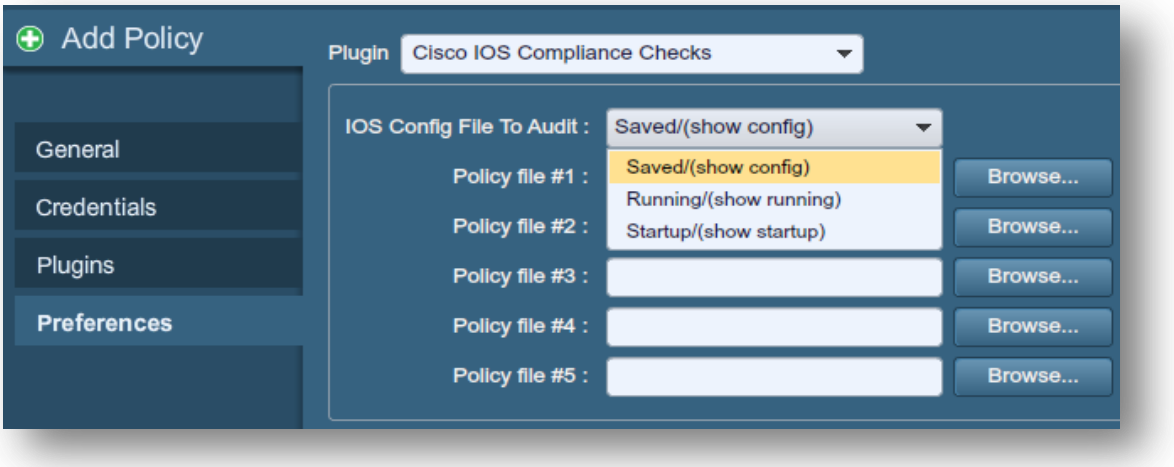
Hinweis: Hostgeräte brauchen für die „ADSI Settings“ und „Apple Profile Manager API Settings“ nicht direkt gescannt zu werden, um ihre Informationen zu erhalten. Der Nessus-Scanner muss den MDM (Mobile Device Management)-Server zwecks Abfrage der Informationen erreichen können. Sofern eine dieser Optionen konfiguriert wurde, erfordert die Scanrichtlinie keinen Zielhost zum Scannen; Sie können „localhost“ als Ziel angeben und die Richtlinie fragt weiterhin den MDM-Server nach den Informationen ab.

Mit „**Apple Profile Manager API Settings**“ fragt Nessus den Apple Profile Manager-Server ab, um eine Enumeration der Apple iOS-basierten Geräte (z. B. iPhone, iPad) im Netzwerk aufzustellen. Nessus führt mithilfe der Anmeldedaten und Serverinformationen eine Authentifizierung auf dem Profile Manager durch, um die Geräteinformationen direkt abzufragen. Optional können Kommunikationen über SSL vorgegeben werden und der Server kann auch angewiesen werden, eine Aktualisierung der Geräteinformationen zu erzwingen (d. h. jedes einzelne Gerät aktualisiert seine Angaben auf dem Profile Manager-Server).

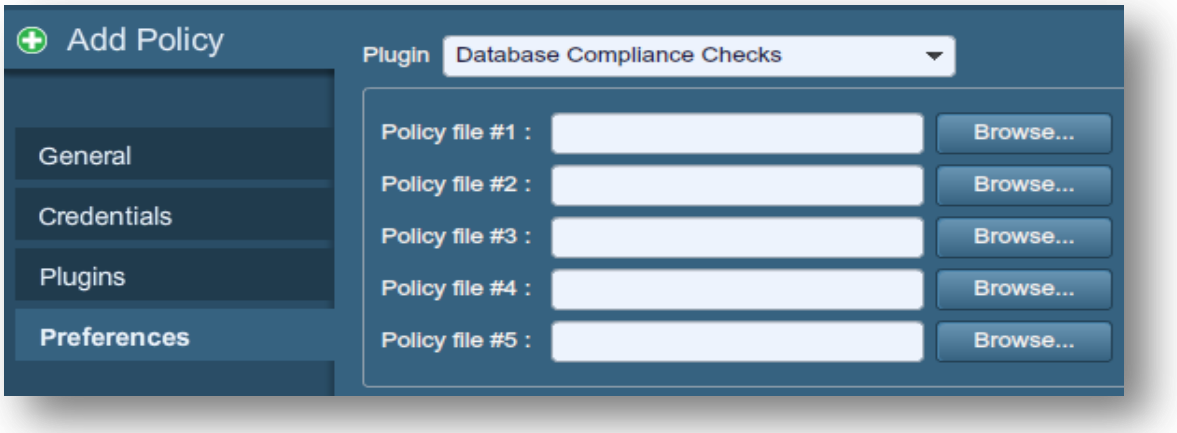
Für diese Funktion müssen keine Ports in der Scanrichtlinie angegeben werden. Die Einstellungen werden für Scans von Mobilgeräten benötigt.



Mit der Option „**Cisco IOS Compliance Checks**“ („Cisco IOS-Compliancetests“) können ProfessionalFeed-Kunden Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes Gerät, das unter Cisco IOS läuft, die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden. Diese Richtlinien können für die gespeicherte Konfiguration (Saved, **`show config`**), die laufende Konfiguration (Running, **`show running`**) oder die Startkonfiguration (Startup, **`show startup`**) ausgeführt werden.



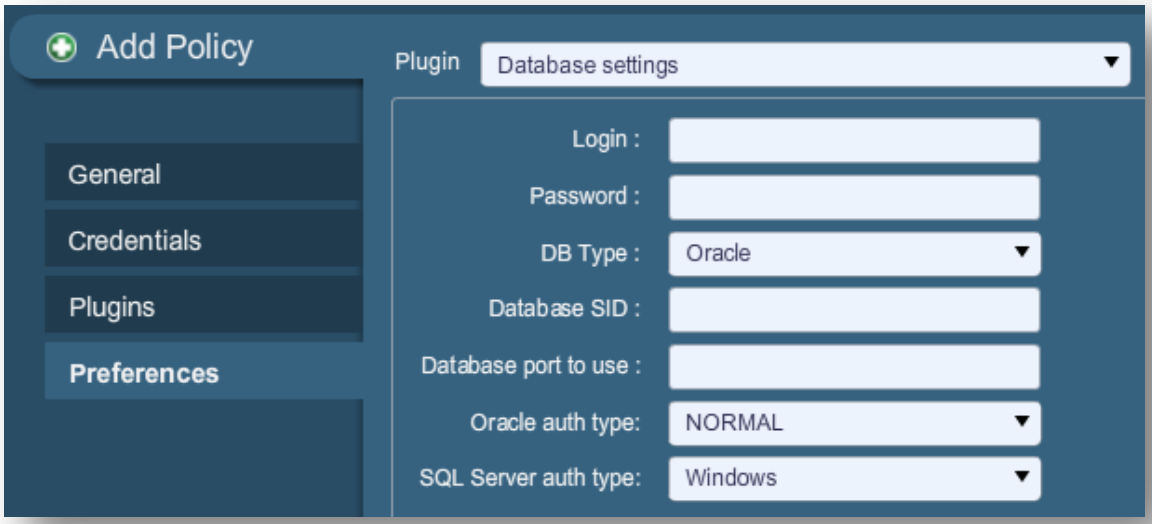
Mit der Option „**Database Compliance Checks**“ („Datenbank-Compliancetests“) können ProfessionalFeed-Kunden Richtliniendateien hochladen, anhand derer ermittelt wird, ob eine getestete Datenbank die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



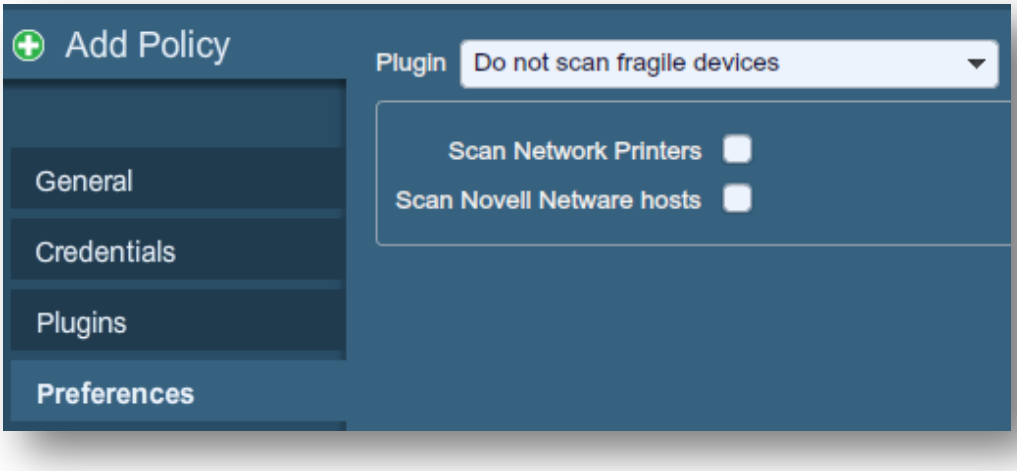
Mithilfe der Optionen unter „**Database settings**“ („Datenbankeinstellungen“) werden der Typ der zu testenden Datenbank, zugehörige Einstellungen und Anmeldedaten angegeben:

Option	Beschreibung
Login (Anmeldename)	Der Benutzername für die Datenbank.
Password (Kennwort)	Das Kennwort zum angegebenen Benutzernamen.
DB Type (Datenbanktyp)	Oracle, SQL Server, MySQL, DB2, Informix/DRDA und PostgreSQL werden unterstützt.
Database SID (System-ID der Datenbank)	ID der zu prüfenden Datenbank.

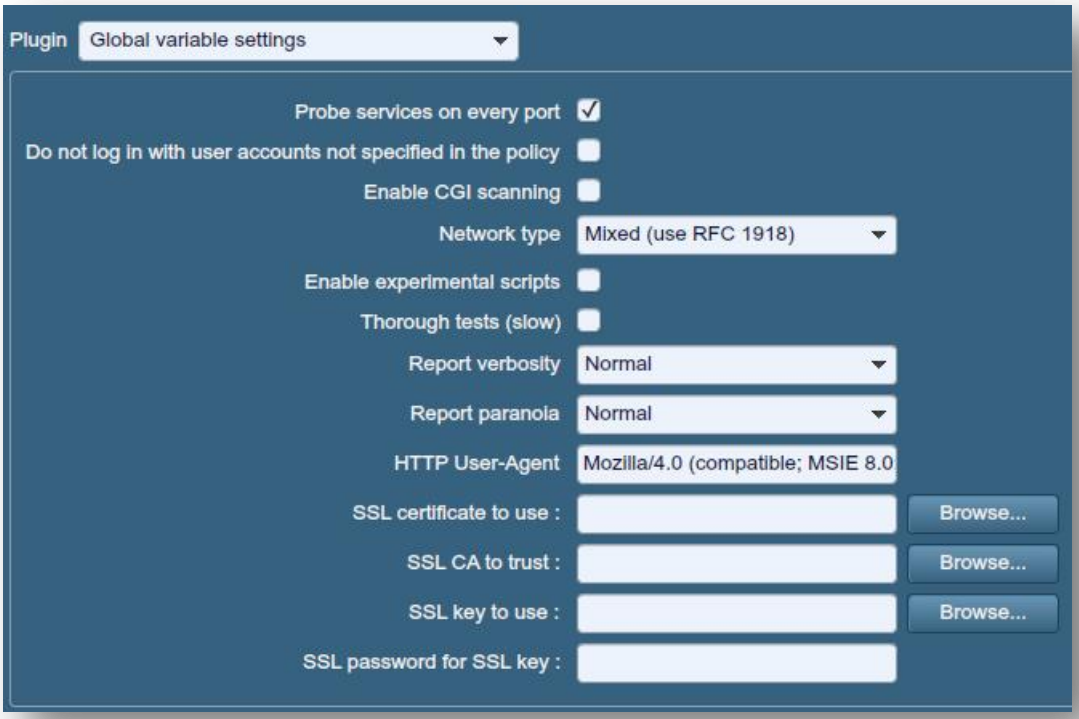
Database port to use (Zu verwendender Datenbankport)	Port, auf dem die Datenbank horcht.
Oracle auth type (Oracle-Authentifizierungstyp)	NORMAL, SYSOPER und SYSDBA werden unterstützt.
SQL Server auth type (SQL Server-Authentifizierungstyp)	Windows und SQL werden unterstützt.



„**Do not scan fragile devices**“ („Anfällige Geräte nicht scannen“) bietet zwei Optionen, um den Nessus-Scanner so zu konfigurieren, dass Hosts, die sich in der Vergangenheit als anfällig erwiesen haben oder bei unerwarteten Eingaben zu Abstürzen neigen, nicht gescannt werden. Mit den Optionen „Scan Network Printers“ („Netzwerkdrucker scannen“) und „Scan Novell Netware hosts“ („Novell Netware-Hosts scannen“) kann festgelegt werden, dass diese Geräte von Nessus gescannt werden. Damit die Geräte gescannt werden, müssen diese Optionen aktiviert sein. Es wird empfohlen, Scans dieser Geräte auf eine Weise durchzuführen, die eine Überwachung der Systeme auf Probleme durch die IT-Mitarbeiter gestattet.



Unter „**Global variable settings**“ („Globale Variableneinstellungen“) ist eine Vielzahl von Konfigurationsoptionen für den Nessus-Server enthalten.

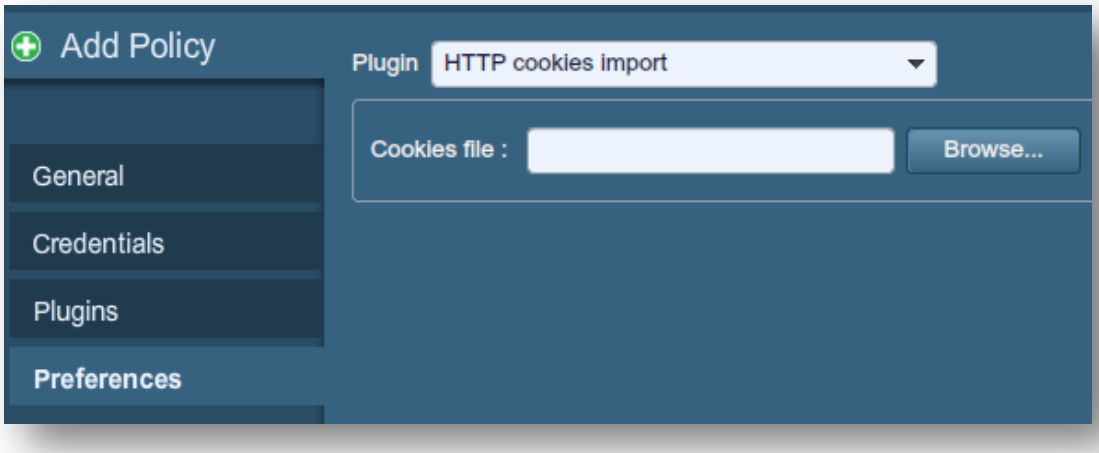


Die folgende Tabelle enthält ausführliche Informationen zu den verfügbaren Optionen:

Option	Beschreibung
Probe services on every port (Dienste auf jedem Port testen)	Bei Auswahl dieser Option wird versucht, jedem offenen Port den Dienst zuzuordnen, der auf diesem Port ausgeführt wird. Beachten Sie, dass es in seltenen Fällen zu Störungen einiger Dienste und zu nicht vorhersehbaren Nebeneffekten kommen kann.
Do not log in with user accounts not specifiedin the policy (Keine Anmeldung mit Benutzerkonten, die in der Richtlinie nicht angegeben sind)	Hiermit werden Kontensperrungen verhindert, wenn Ihre Kennwortrichtlinie vorsieht, dass Konten nach mehreren ungültigen Anmeldeversuchen gesperrt werden.
Enable CGI scanning (CGI-Scans aktivieren)	Hiermit werden CGI-Tests aktiviert. Durch Deaktivierung dieser Option wird ein Audit eines lokalen Netzwerks ganz erheblich beschleunigt.
Network type (Netzwerktyp)	Hier können Sie angeben, ob Sie öffentliche oder private IP-Adressen oder eine Kombination dieser beiden Typen verwenden. Wählen Sie „Mixed“ („Gemischt“) aus, wenn Sie RFC 1918-Adressen verwenden und mehrere Router in Ihrem Netzwerk einsetzen.
Enable experimental scripts (Experimentelle Skripts verwenden)	Gestattet die Verwendung von als experimentell betrachteten Plugins für den Scan. Lassen Sie diese Option deaktiviert, wenn Sie ein Produktionsnetzwerk scannen.

Thorough tests (slow) **(Umfassende Tests, langsam)**	Wenn Sie diese Option aktivieren, wird die Testleistung bestimmter Plugins erhöht. Wenn Sie beispielsweise SMB-Dateifreigaben überprüfen, wird ein entsprechendes Plugin bei aktivierter Option eine Analysetiefe von drei Stufen (statt einer Stufe) verwenden. In bestimmten Fällen kann die Auswahl dieser Option sowohl die Analyse verlängern als auch das Datenaufkommen im Netzwerk erheblich erhöhen. Beachten Sie auch, dass umfassende Scans aggressiver vorgehen und Störungen im Netzwerk wahrscheinlicher sind; dafür sind die Auditergebnisse aussagekräftiger.
Report verbosity **(Berichtsausführlichkeit)**	Je höher der hier zugewiesene Wert, desto mehr Informationen zu Plugin-Aktivitäten werden in den Bericht aufgenommen.
Report paranoia **(Maximale Sicherheit im Bericht)**	In einigen Fällen kann von Nessus remote nicht bestimmt werden, ob tatsächlich ein Schwachpunkt vorliegt. Wenn Sie für diese Optionen die Einstellung „**Paranoid**“ auswählen, wird in jedem Fall ein Schwachpunkt gemeldet, auch wenn ein Fehlalarm nicht ausgeschlossen werden kann. Umgekehrt führt die Einstellung „**Avoid false alarm**“ („ Fehlalarme vermeiden“) dazu, dass Nessus einen Schwachpunkt nicht meldet, wenn nicht sicher ist, dass er vorhanden ist. Die Standardoption („**Normal**“) stellt einen Kompromiss zwischen den vorgenannten beiden Einstellungen dar.
HTTP User-Agent	Hiermit wird angegeben, welchen Webbrowsertyp Nessus beim Scannen emuliert.
SSL certificate to use **(Zu verwendendes SSL-Zertifikat)**	Ermöglicht Nessus die Verwendung eines clientseitigen SSL-Zertifikats für die Kommunikation mit einem Remotehost.
SSL CA to trust **(Vertrauenswürdige SSL-Zertifizierungsstelle)**	Hier wird eine Zertifizierungsstelle (Certificate Authority, CA) angegeben, die Nessus als vertrauenswürdig einstuft.
SSL key to use **(Zu verwendender SSL-Schlüssel)**	Hiermit wird ein lokaler SSL-Schlüssel zur Verwendung für die Kommunikation mit dem Remotehost angegeben.
SSL password for SSL key **(SSL-Kennwort für SSL-Schlüssel)**	Hier geben Sie das Kennwort zur Verwaltung des angegebenen SSL-Schlüssels an.

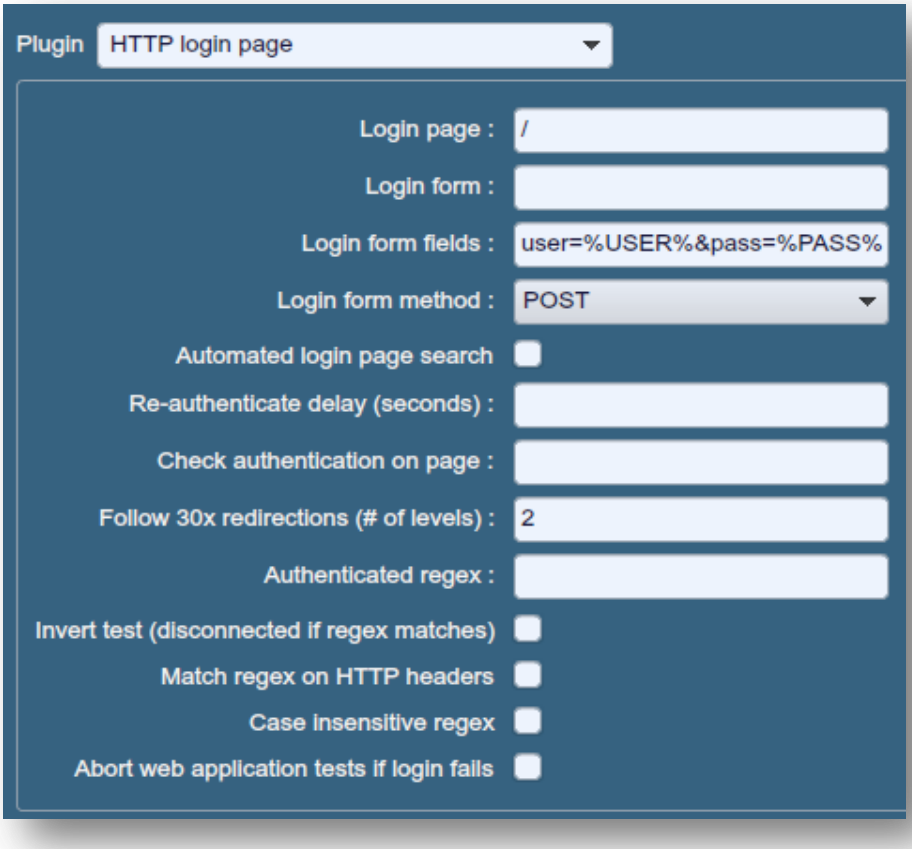
Zur Erleichterung von Webanwendungstests kann Nessus HTTP-Cookies aus einer anderen Software (z. B. Webbrowser, Webproxy usw.) importieren. Der Import wird mit den Einstellungen unter „**HTTP cookies import**“ (HTTP-Cookieimport) gesteuert. Eine Cookiedatei kann hochgeladen werden, damit Nessus die Cookies für den Zugriff auf eine Webanwendung verwendet. Die Cookiedatei muss im Netscape-Format vorliegen.



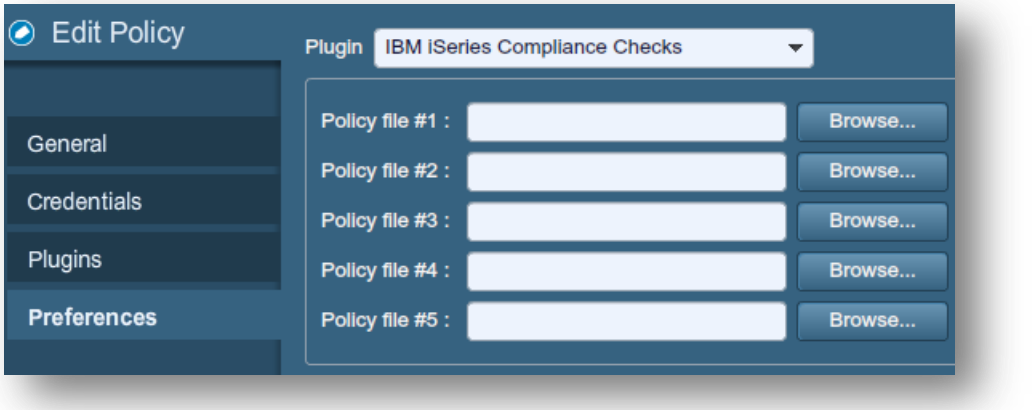
Mit den Einstellungen unter „**HTTP login page**“ („HTTP-Anmeldeseite“) können Sie festlegen, an welcher Stelle authentifizierte Tests einer benutzerdefinierten webbasierten Anwendung beginnen.

Option	Beschreibung
Login page (Anmeldeseite)	Dies ist die Basis-URL der Anmeldeseite der Anwendung.
Login form (Anmeldeformular)	Dies ist der Parameter „action“ für die Formularmethode. Beispielsweise würde bei `<form method="POST" name="auth_form" action="/login.php">` der Wert „`/login.php`“ heißen.
Login form fields (Anmeldeformularfelder)	Geben Sie die Authentifizierungsparameter (z. B. `login=%USER%&password=%PASS%`) ein. Wenn die Schlüsselwörter %USER% und %PASS% verwendet werden, werden diese durch die Werte ersetzt, die im Dropdownmenü „Login configurations“ („Anmeldekonfiguration“) angegeben wurden. Mithilfe dieses Feldes können, falls erforderlich, auch zwei Parameter angegeben werden (z. B. ein „Gruppenname“ oder eine andere Information, die für den Authentifizierungsprozess erforderlich ist).
Login form method (Anmeldeformularmethode)	Geben Sie an, ob die Anmeldeaktion über eine GET- oder eine POST-Anforderung erfolgt.
Automated login page search (Automatische Suche der Anmeldeseite)	Hiermit wird Nessus angewiesen, nach einer Anmeldeseite zu suchen.
Re-authenticate delay (seconds) (Verzögerung für Neuauthentifizierung, in Sekunden)	Zeitliche Verzögerung bis zum nächsten Authentifizierungsversuch. Dieser Parameter ist nützlich, um das Auslösen von Schutzmechanismen gegen Brute-Force-Angriffe zu vermeiden.
Check authentication on page (Authentifizierung auf der Seite überprüfen)	Hier wird die URL einer geschützten Webseite angegeben, die eine Authentifizierung erfordert. Auf diese Weise kann Nessus den Authentifizierungsstatus einfacher feststellen.
Follow 30x redirections (# of levels) (30x-Umleitungen folgen, Anzahl der Ebenen)	Wenn ein 30x-Umleitungscode von einem Webserver empfangen wird, wird hier festgelegt, ob dieser Nessus an den angegebenen Link weiterleitet.

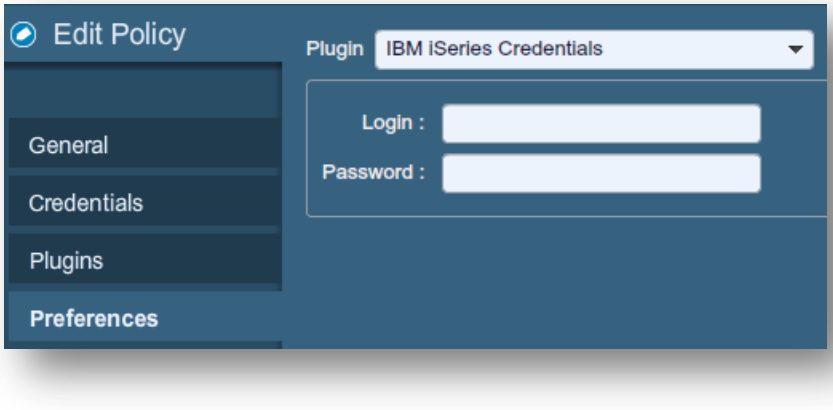
Authenticated regex (Authentifizierter regulärer Ausdruck)	Ein regulärer Ausdruck, nach dem auf der Anmeldeseite gesucht werden soll. Manchmal ist es zur Feststellung des Sitzungsstatus nicht ausreichend, einfach nur einen 200-Antwortcode zu erhalten. Nessus kann versuchen, einen Vergleich auf Vorhandensein eines angegebenen Strings wie beispielsweise „Authentication successful!“ („Authentifizierung erfolgreich“) durchzuführen.
Invert test (disconnected if regex matches) (Test umkehren (Trennung bei Übereinstimmung mit regulärem Ausdruck)	Ein regulärer Ausdruck, nach dem auf der Anmeldeseite gesucht wird. Wenn die Suche erfolgreich ist, wird Nessus mitgeteilt, dass die Authentifizierung fehlgeschlagen ist (Beispiel: „Authentication failed!“)
Match regex on HTTP headers (HTTP-Header mit regulärem Ausdruck vergleichen)	Anstelle des Datenteils einer HTTP-Antwort kann Nessus auch die Header (Kopfdaten) der Antwort nach einem gegebenen regulären Ausdruck durchsuchen, um den Authentifizierungsstatus besser ermitteln zu können.
Case insensitive regex (Keine Unterscheidung der Groß-/Kleinschreibung bei regulären Ausdrücken)	Bei Suchvorgängen mit regulären Ausdrücken wird die Groß-/Kleinschreibung standardmäßig beachtet. Mit dieser Option können Sie Nessus anweisen, die Groß-/Kleinschreibung zu ignorieren.
Abort web application tests if login fails (Bei fehlgeschlagener Anmeldung Webanwendungstests abbrechen)	Wenn die angegebenen Anmeldedaten nicht funktionieren, bricht Nessus die benutzerdefinierten Webanwendungstests ab (nicht jedoch die CGI-Plugin-Familien).



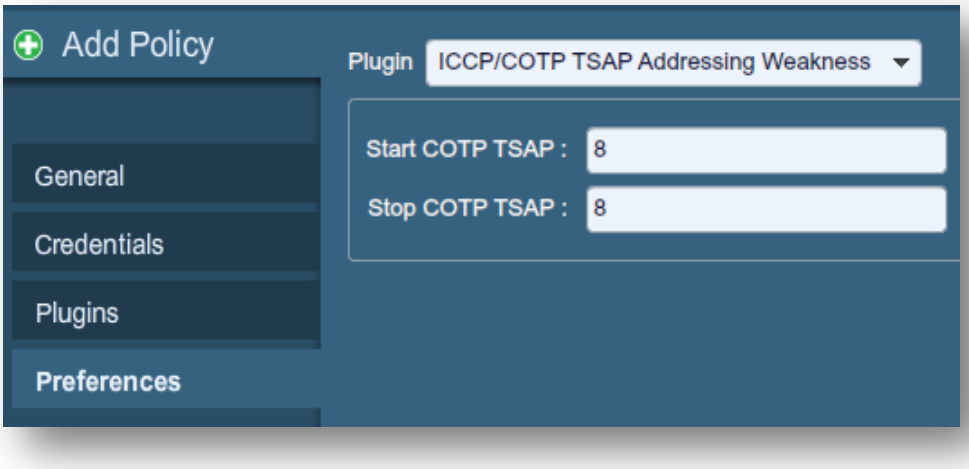
Mit der Option „**IBM iSeries Compliance Checks**“ („IBM iSeries-Compliancetests“) können ProfessionalFeed-Kunden Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes IBM iSeries-System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



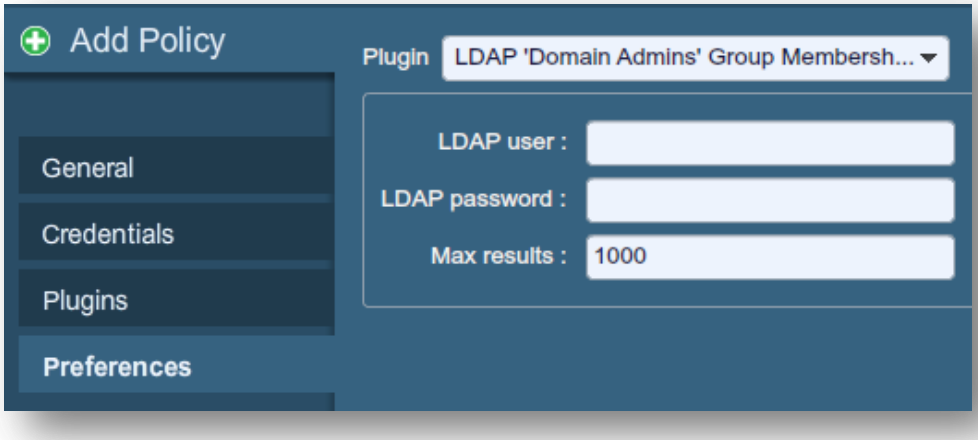
Die Einstellung „**IBM iSeries Credentials**“ („IBM iSeries-Anmeldedaten“) ermöglicht die Übergabe von Nessus-Anmeldedaten zur Authentifizierung bei einem IBM iSeries-System. Dies ist beispielsweise für Compliance-Audits erforderlich.



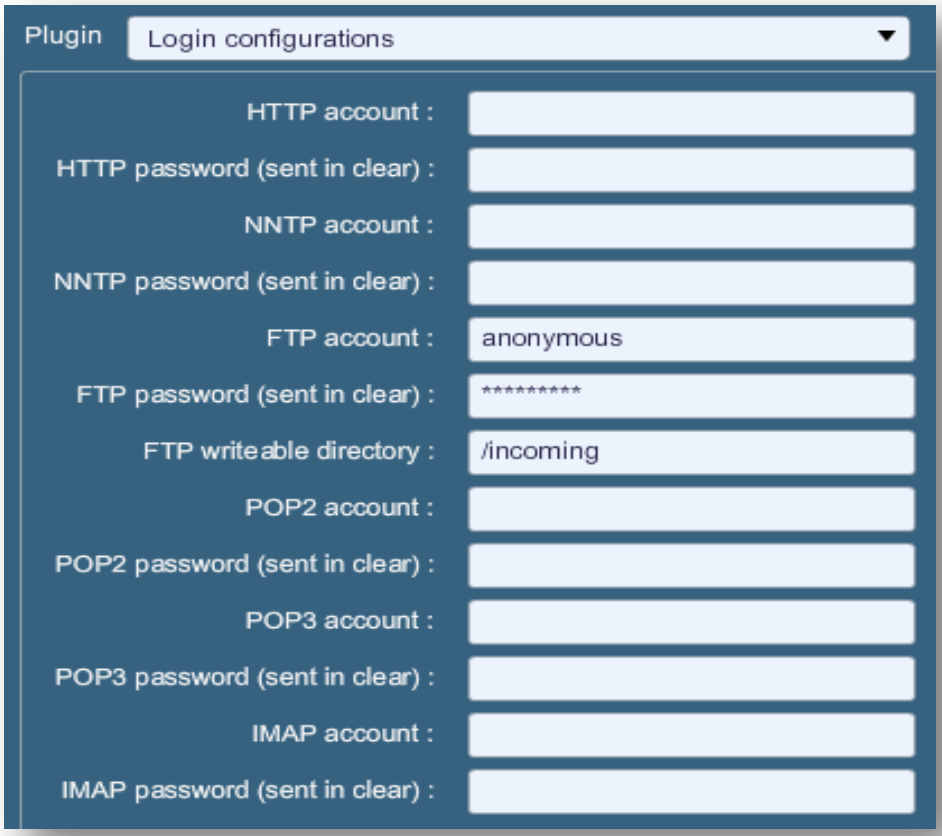
Das Menü „**ICCP/COTP TSAP Addressing**“ („ICCP/COTP-TSAP-Adressierung“) dient vor allem der Konfiguration von SCADA-Tests. Es bestimmt durch Ausprobieren möglicher Werte einen COTP-TSAP-Wert (Connection Oriented Transport Protocol/Transport Service Access Points) auf einem ICCP-Server. Die Start- und Stoppwerte sind standardmäßig auf „8“ festgelegt.



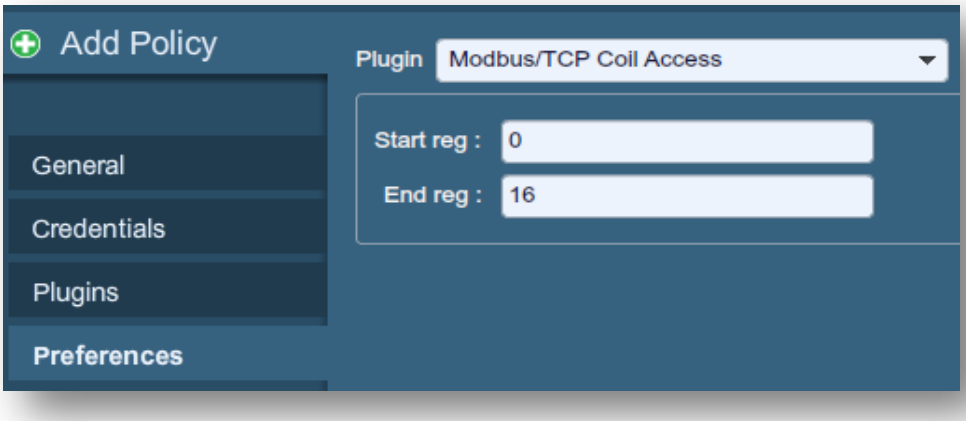
Im Menü „LDAP ‘Domain Admins’ Group Membership Enumeration“ („Auflistung der Mitgliedschaften in der LDAP-Gruppe, Domain Admins“) können Sie LDAP-Anmeldedaten eingeben, mit denen Sie eine Liste der Mitglieder der Gruppe „Domain Admins“ in einem entfernten LDAP-Verzeichnis erstellen.



Mit „**Login configurations**“ („Anmeldekonfigurationen“) wird dem Nessus-Scanner die Verwendung von Anmeldedaten beim Testen von HTTP, NNTP, FTP, POP2, POP3 oder IMAP ermöglicht. Wenn Anmeldedaten angegeben werden, kann Nessus ausführlichere Tests zur Erkennung von Sicherheitslücken ausführen. Hier angegebene HTTP-Anmeldedaten werden nur für die Basis- und die Digest-Authentifizierung verwendet. Verwenden Sie zur Konfiguration der Anmeldedaten für eine angepasste Webanwendung das Pulldownmenü „HTTP login page“ („HTTP-Anmeldeseite“).

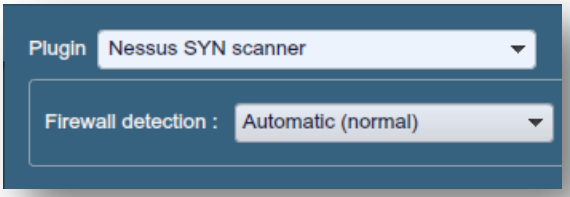


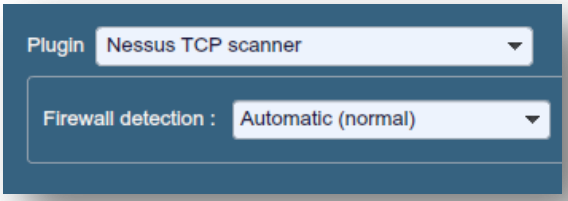
Die Optionen unter „**Modbus/TCP Coil Access**“ („Modbus-/TCP-Coil-Zugriff“) stehen nur ProfessionalFeed-Benutzern zur Verfügung. Dieses Dropdownmenü wird durch die SCADA-Plugins, die Bestandteil des ProfessionalFeed sind, dynamisch generiert. Modbus verwendet den Funktionscode „1“ zum Auslesen der „Coils“ auf einem Modbus-Slave. Coils stellen binäre Ausgabeeinstellungen dar und sind gewöhnlich Auslösern zugeordnet. Durch Auslesen von Coils kann ein Angreifer möglicherweise ein Systemprofil erstellen und Registerbereiche erkennen, die er dann über einen Write-Coil-Befehl ändern kann. Die Standardwerte sind „0“ für das Start-Register und „16“ für das End-Register.



Mit den Optionen „**Nessus SYN scanner**“ und „**Nessus TCP scanner**“ können Sie die Erkennung einer Firewall durch die nativen SYN- bzw. TCP-Scanner verbessern.

Wert	Beschreibung
Automatic (normal) (Automatisch (normal))	Durch Einstellung dieser Option kann einfacher erkannt werden, ob sich eine Firewall zwischen dem Scanner und dem Zielsystem befindet (**Standard**).
Disabled (softer) (Inaktiv (weniger aggressiv))	Hierdurch wird die Funktion **Firewall detection** („Firewallerkennung“) deaktiviert.
Do not detect RST rate limitation (soft) (RST-Ratenbeschränkung nicht erkennen (weniger aggressiv))	Hiermit wird die Möglichkeit deaktiviert, festzustellen, wie häufig Resets festgelegt werden und ob auf einem nachgeschalteten Netzwerkgerät eine Beschränkung konfiguriert ist.
Ignore closed ports (aggressive) (Geschlossene Ports ignorieren (aggressiv))	Hierbei wird versucht, Plugins auch dann auszuführen, wenn der Port geschlossen zu sein scheint. Es wird nicht empfohlen, diese Option in einem Produktionsnetzwerk einzusetzen.

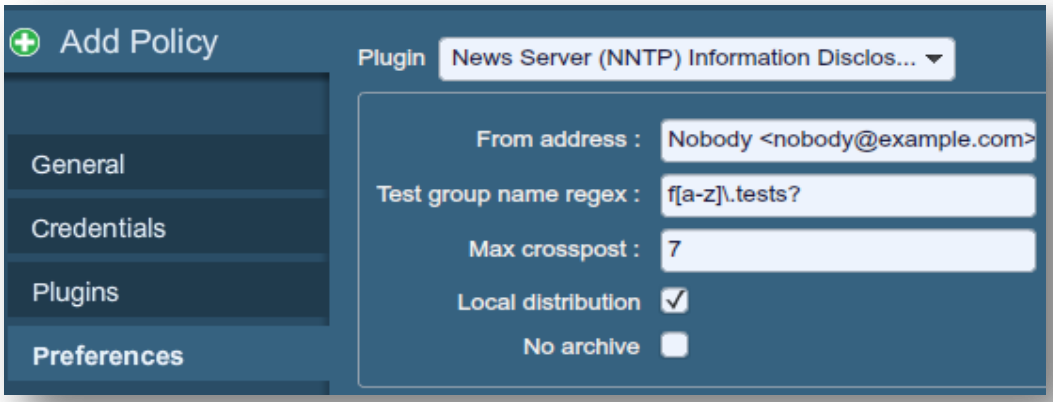




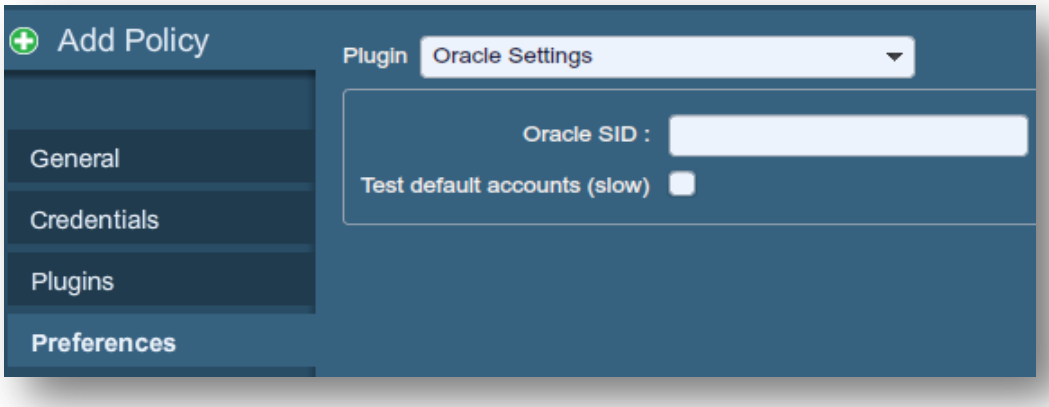
Mithilfe der Option „**News Server (NNTP) Information Disclosure**“ („Offenlegung von Newsserver-(NNTP-)Daten“) kann bestimmt werden, ob vorhandene Newsserver zur Weiterleitung von Spam verwendet werden. Nessus versucht, einen Newsbeitrag an einen oder mehrere NNTP-Server (Network News Transport Protocol) zu schicken, und kann dann überprüfen, ob es möglich ist, diesen Beitrag auch an nachgeschaltete Newsserver zu schicken.

Option	Beschreibung
From address (Absenderadresse)	Adresse, die von Nessus für den Versand eines Beitrags an den oder die Newsserver verwendet wird. Der Beitrag selbst wird nach kurzer Zeit automatisch gelöscht.
Test group name regex (Regulärer Ausdruck für Namen der Testgruppen)	Name der Newsgroup(s), die einen Testbeitrag von der angegebenen Adresse erhalten. Der Name kann als regulärer Ausdruck angegeben werden, sodass der Beitrag an mehrere Newsgroups gleichzeitig gesendet werden kann. Beispielsweise wird beim Standardwert „**f[a-z]\.tests?**“ ein Beitrag an alle Newsgroups gesendet, deren Name mit einem beliebigen Buchstaben (zwischen „a“ und „z“) beginnt und in „.tests“ (oder eine dem String entsprechende Abwandlung) endet. Das Fragezeichen dient als optionaler Platzhalter.
Max crosspost (Weiterleitungen maximal)	Maximale Anzahl von Newsservern, die unabhängig von Namensübereinstimmungen den Testbeitrag erhalten. Wenn hier etwa der Wert „**7**“ festgelegt wird, wird der Testbeitrag nur an sieben Newsserver gesendet, und zwar auch dann, wenn womöglich 2000 Newsserver dem regulären Ausdruck in diesem Feld entsprechen.

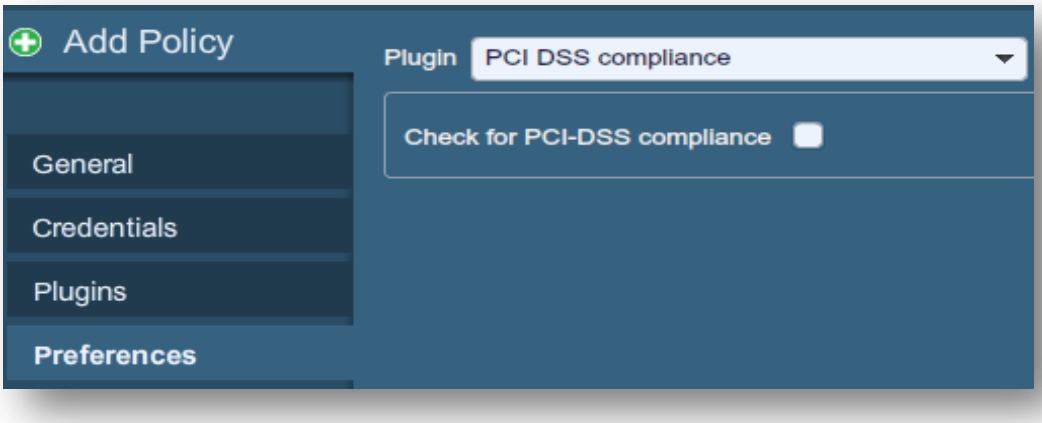
Local distribution (Lokale Übermittlung)	Wenn diese Option ausgewählt ist, sendet Nessus den Testbeitrag nur an lokale Newsserver. Andernfalls wird versucht, den Beitrag auch an nachgeschaltete Systeme weiterzuleiten.
No archive (Keine Archivierung)	Wenn diese Option ausgewählt ist, fordert Nessus an, dass der Testbeitrag auf dem oder den Newsservern nicht archiviert wird. Andernfalls wird der Beitrag wie jeder andere auch archiviert.



Unter „**Oracle Settings**“ („Oracle-Einstellungen“) wird in Nessus die Oracle Database SID konfiguriert. Außerdem wird eine Option zum Testen auf bekannte Standardkonten in der Oracle-Software hinzugefügt.



Bei Auswahl von „**PCI DSS Compliance**“ („PCI-DSS-Compliance“) kann Nessus die Scanresultate mit den aktuellen Vorgaben für die PCI-DSS-Compliance vergleichen. Diese Funktion steht nur ProfessionalFeed-Kunden zur Verfügung.



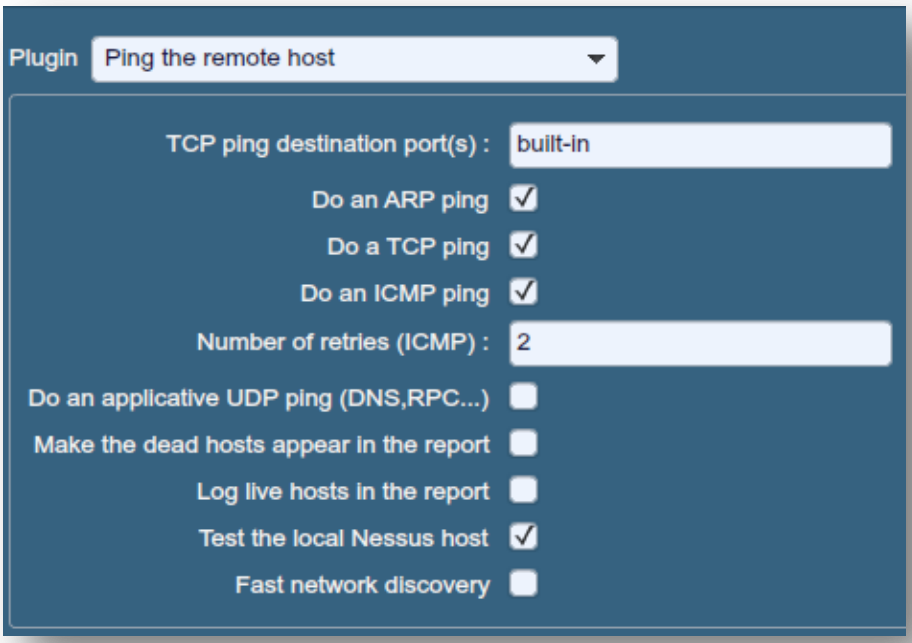
Nessus verarbeitet Anmeldedaten für die Patchmanagementsysteme Red Hat Satellite Server, WSUS, SCCM und VMware Go (vormals Shavlik), um Patch-Audits auf Systemen auszuführen, für die Nessus nicht über geeignete Anmeldedaten verfügt. Optionen für diese Patchmanagementsysteme sind in den entsprechenden Dropdownmenüs auf der Seite „Preferences“ vorhanden: „**Patch Management: Red Hat Satellite Server Settings**“, „**Patch Management: SCCM Server Settings**“, „**Patch Management: VMware Go Server Settings**“ und „**Patch Management: WSUS Server Settings**“. Weitere Informationen zur Verwendung von Nessus, um Hosts mithilfe dieser Patchmanagementsysteme zu scannen, entnehmen Sie dem Dokument „Patch Management Integration“.

Mit den Optionen unter „**Ping the remote host**“ („Pingbefehl an Remotehost senden“) lassen sich die Funktionen zum Versenden von Pingbefehlen an Hosts durch Nessus während des Erkennungsscans sehr genau konfigurieren. Es können ARP-Pings, TCP-Pings, ICMP-Pings oder geeignete UDP-Pings verwendet werden.

Option	Beschreibung
TCP ping destination port(s) (Zielport(s) für TCP-Pings)	Gibt die Liste der Ports an, die über einen TCP-Ping überprüft werden. Wenn Sie nicht sicher sind, welche Ports Sie angeben sollen, lassen Sie die Voreinstellung „built-in“ („Integriert“) stehen.
Number of Retries (ICMP) (Anzahl der Wiederholungen (ICMP))	Hiermit können Sie festlegen, wie oft die Übermittlung von Pingbefehlen an den Remotehost probiert wird. Der Standardwert ist „6“.
Do an applicative UDP ping (DNS, RPC…) (Geeigneten UDP-Ping ausführen (DNS, RPC …))	Hiermit wird ein UDP-Ping für bestimmte UDP-basierte Anwendungen wie DNS (Port 53), RPC (Port 111), NTP (Port 123) oder RIP (Port 520) ausgeführt.
Make the dead hosts appear in the report (Tote Hosts im Bericht aufführen)	Wenn diese Option aktiviert ist, werden Hosts, die auf die Pinganforderung nicht reagiert haben, als „tote“ Hosts im Sicherheitsbericht aufgeführt.
Log live hosts in the report (Hosts, die online sind, im Bericht protokollieren)	Wählen Sie diese Option aus, um im Bericht gezielt aufzuführen, an welche Remotehosts erfolgreich ein Pingbefehl gesendet werden konnte.
Test the local Nessus host (Lokalen Nessus-Host testen)	Mithilfe dieser Option können Sie den lokalen Nessus-Host in den Scan einschließen bzw. daraus ausschließen. Die Option wird angewendet, wenn der Nessus-Host in den Bereich des für den Scan konfigurierten Zielnetzwerks fällt.

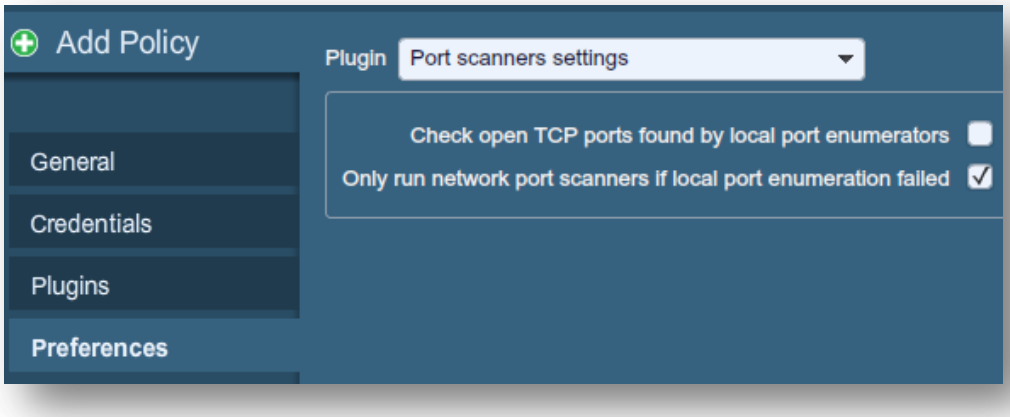
Fast network discovery (Schnelle Netzwerkerkennung)	Standardmäßig werden, wenn Nessus einen Pingbefehl an eine entfernte IP-Adresse sendet und eine Antwort erhält, zusätzliche Tests durchgeführt, um sicherzustellen, dass es sich nicht um einen transparenten Proxy oder ein Lastausgleichsmodul handelt, von denen statt einer Antwort nur sinnlose Daten zurückgegeben werden (einige Geräte antworten auf jedem Port zwischen 1 und 65.535, auch wenn der betreffende Port von keinem Dienst verwendet wird). Solche Tests können insbesondere dann einige Zeit in Anspruch nehmen, wenn sich der Remotehost hinter einer Firewall befindet. Ist die Option „Fast network discovery“ aktiviert, dann werden diese Tests von Nessus nicht ausgeführt.

Zum Scannen von VMware-Gastsystemen muss „ping“ deaktiviert sein. Deaktivieren Sie in diesem Fall die Einträge für TCP-, ICMP- und ARP-Pings für die Sicherheitsrichtlinie „Advanced“ > „Ping the remote host“.


Plugin
Ping the remote host
TCP ping destination port(s) :
built-in
Do an ARP ping
Do a TCP ping
Do an ICMP ping
Number of retries (ICMP) :
2
Do an applicative UDP ping (DNS,RPC...)
Make the dead hosts appear in the report
Log live hosts in the report
Test the local Nessus host
Fast network discovery

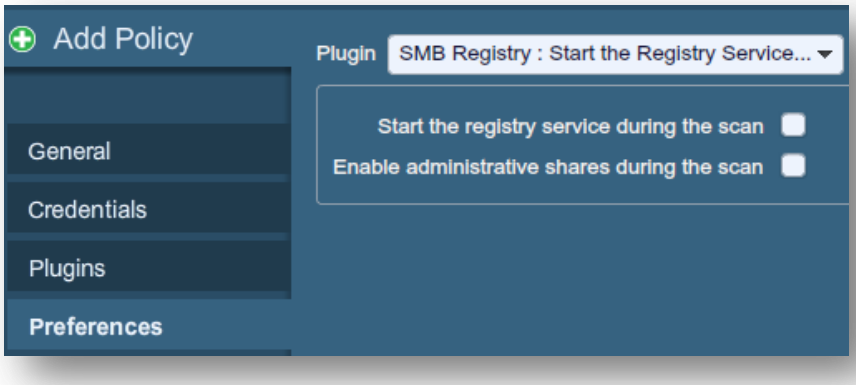
Unter „**Port scanner settings**“ („Portscannereinstellungen“) sind zwei Optionen für die weitere Steuerung der Portscanneraktivitäten enthalten:

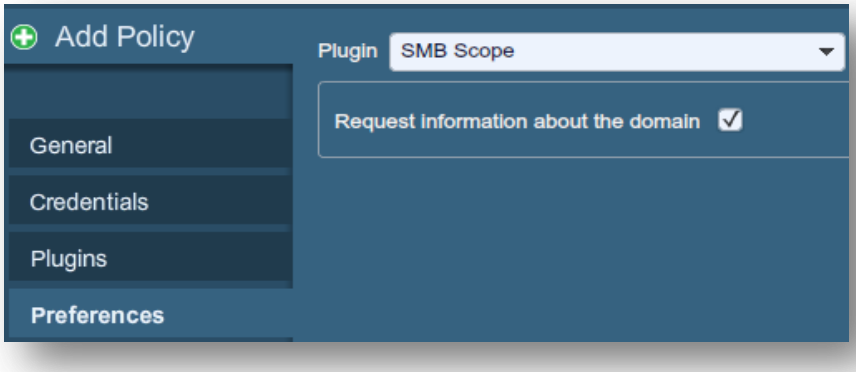
Option	Beschreibung
Check open TCP ports found by local port enumerators (Offene TCP-Ports überprüfen, die von lokalen Port-Enumeratoren gefunden wurden)	Wenn ein lokaler Port-Enumerator (z. B. WMI oder netstat) einen Port erkennt, überprüft Nessus auch, ob dieser Port für Remoteverbindungen geöffnet ist. Auf diese Weise kann festgestellt werden, ob irgendeine Form der Zugriffssteuerung (z. B. TCP-Wrappers, Firewall) verwendet wird.
Only run network port scanners if local port enumeration failed (Netzwerkportscanner nur ausführen, wenn die lokale Port-Enumeration fehlgeschlagen ist)	Andernfalls wird zunächst auf die lokale Port-Enumeration zurückgegriffen.



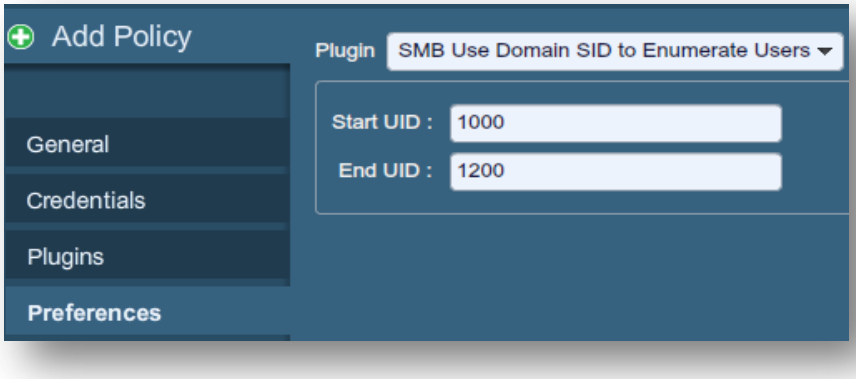
Mit „**SMB Registry: Start the Registry Service during the scan**“ („SMB-Registrierung: Registrierungsdienst während des Scans starten“) kann der Dienst aktiviert werden, um einige Scanvoraussetzungen auf Computern zu erfüllen, auf denen die SMB-Registrierung nicht fortlaufend ausgeführt wird.

Im Menü „**SMB Scope**“ („SMB-Umfang“) werden anstelle lokaler Benutzer Domänenbenutzer abgefragt, sofern die Option „**Request information about the domain**“ („Informationen zur Domäne anfordern“) festgelegt ist.

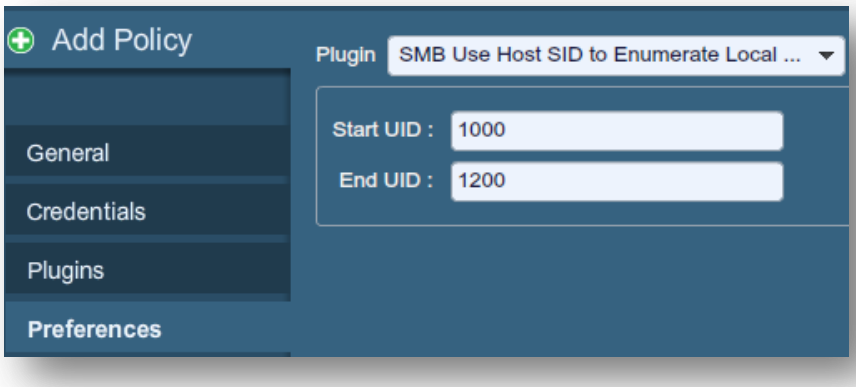




Unter „**SMB Use Domain SID to Enumerate Users**“ („Bei SMB Domänen-SID zur Enumeration von Benutzern verwenden“) wird der SID-Bereich angegeben, für den eine Umkehrsuche (Reverse Lookup) von Benutzernamen in der Domäne ausgeführt wird. Für die meisten Scans wird die Standardeinstellung empfohlen.



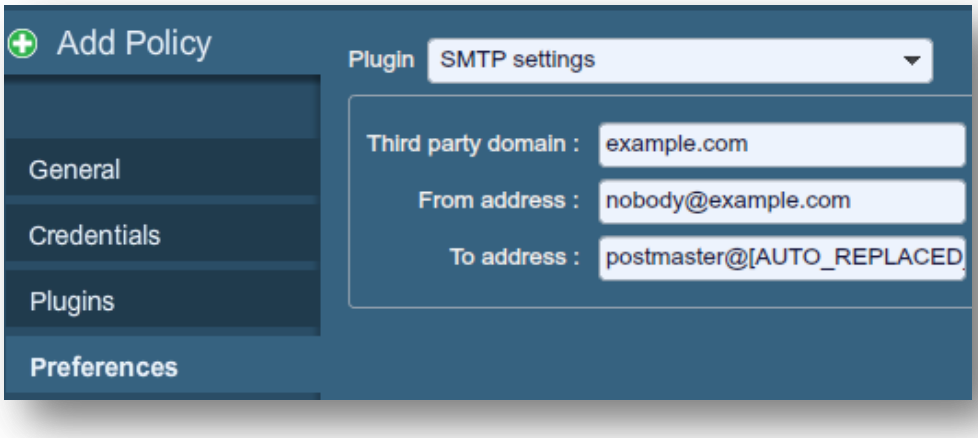
Unter „**SMB Use Host SID to Enumerate Users**“ („Bei SMB Host-SID zur Enumeration von Benutzern verwenden“) wird der SID-Bereich angegeben, für den eine Umkehrsuche (Reverse Lookup) lokaler Benutzernamen ausgeführt wird. Die Verwendung der Voreinstellung wird empfohlen.



Unter „**SMTP settings**“ („SMTP-Einstellungen“) werden Optionen für SMTP-Tests (Simple Mail Transport Protocol) angegeben, die auf allen Geräten innerhalb der gescannten Domäne ausgeführt werden, auf denen SMTP-Dienste laufen. Nessus versucht dabei, Meldungen über das Gerät an die unter „**Third party domain**“ angegebene Fremddomäne weiterzuleiten. Wird die an die Fremddomäne gesendete Nachricht von der im Feld „**To address**“ angegebenen Adresse abgewiesen, dann ist der Spamversuch fehlgeschlagen. Wird die Nachricht hingegen akzeptiert, dann wurde der SMTP-Server erfolgreich zur Weiterleitung von Spam verwendet.

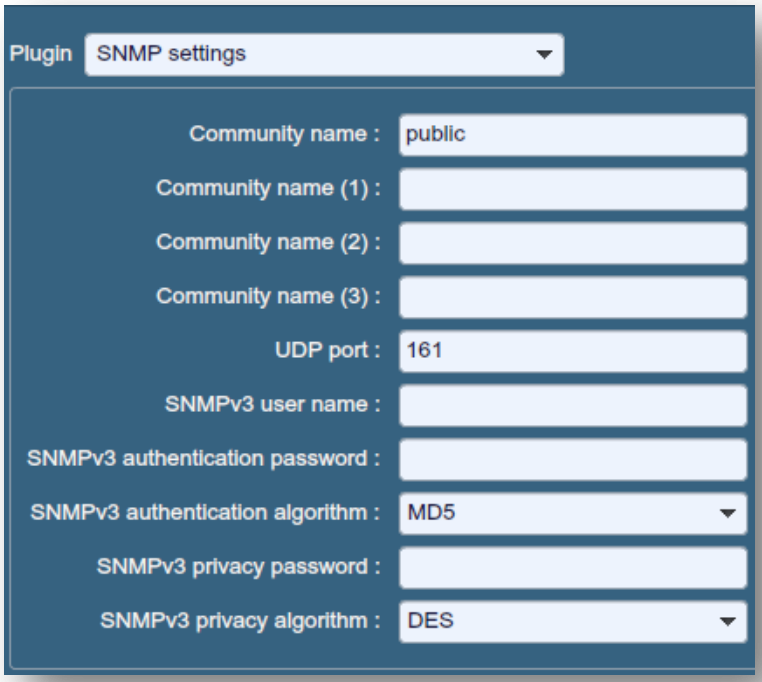
Option	Beschreibung
Third party domain (Fremddomäne)	Nessus versucht, Spam über jedes SMTP-Gerät an die in diesem Feld aufgeführte Adresse zu schicken. Die Adresse dieser Fremddomäne muss außerhalb des Bereichs der Site liegen, die gescannt wird bzw. den Scan ausführt. Andernfalls wird der Test durch den SMTP-Server abgebrochen.
From address (Absenderadresse)	Die an den oder die SMTP-Server gesendeten Testnachrichten geben vor, von der in diesem Feld angegebenen Adresse zu stammen.

To address (Empfängeradresse)	Nessus versucht, Nachrichten an die in diesem Feld aufgeführte Empfängeradresse zu schicken. Vorgegeben ist die Adresse **postmaster**, da sie auf den meisten Mailservern gültig ist.

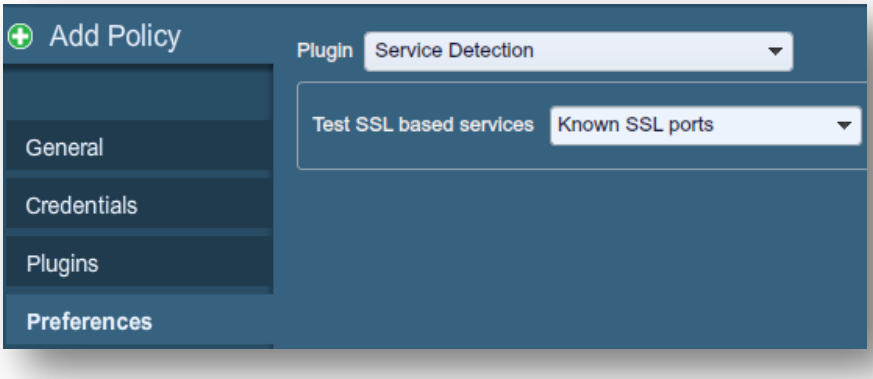


Unter „**SNMP settings**“ („SNMP-Einstellungen“) können Sie Nessus für die Herstellung einer Verbindung mit und die Authentifizierung beim SNMP-Dienst auf dem Zielsystem konfigurieren. Im Verlauf des Scans wird Nessus einige Versuche durchführen, den Community-String zu erraten und für nachfolgende Tests zu verwenden. Je Scanrichtlinie werden bis zu vier separate Community-Strings unterstützt. Kann Nessus den Community-String und/oder das Kennwort nicht erraten, dann kann kein vollständiger Audit des Dienstes ausgeführt werden.

Option	Beschreibung
Community name (0-3) (Community-Name (0-3))	SNMP-Community-Name.
UDP port (UDP-Port)	Weist Nessus an, den Scan über einen anderen Port auszuführen. Vorgesehen für Fälle, in denen SNMP über einen anderen Port als 161 ausgeführt wird.
SNMPv3 user name (SNMPv3-Benutzername)	Benutzername eines SNMPv3-Kontos.
SNMPv3 authentication password (SNMPv3-Authentifizierungskennwort)	Das Kennwort zum angegebenen Benutzernamen.
SNMPv3 authentication algorithm (SNMPv3-Authentifizierungsalgorithmus)	Wählen Sie je nach vom Remotedienst unterstützten Algorithmus MD5 oder SHA1 aus.
SNMPv3 privacy password (SNMPv3-Datenschutzkennwort)	Kennwort, mit dem die verschlüsselte SNMP-Kommunikation geschützt wird.
SNMPv3 privacy algorithm (SNMPv3-Datenschutzalgorithmus)	Der für den SNMP-Datenverkehr verwendete Verschlüsselungsalgorithmus.

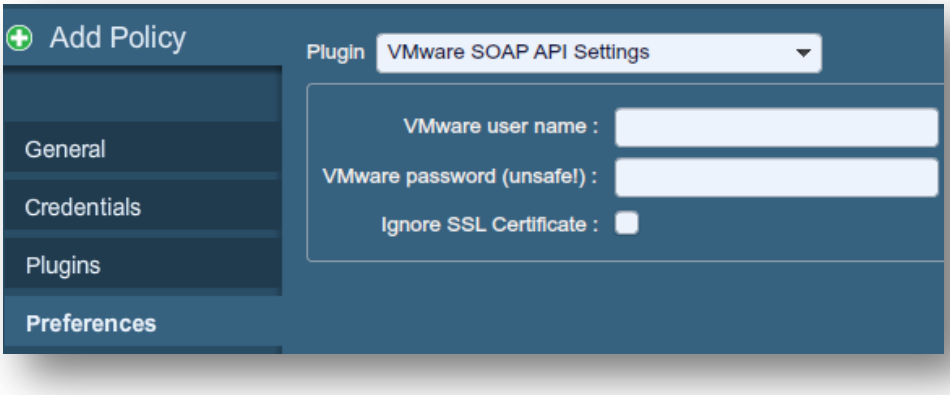


Über „**Service Detection**“ („Diensterkennung“) wird gesteuert, wie Nessus SSL-Dienste testet. Hier können Sie festlegen, ob die Tests für bekannte SSL-Ports (z. B. 443), alle Ports oder gar nicht ausgeführt wird. Das Testen der SSL-Funktionalität auf allen Ports kann auf dem getesteten Host zu einer Betriebsunterbrechung führen.



Mit der Option „**Unix Compliance Checks**“ („UNIX-Compliancetests“) können ProfessionalFeed-Kunden UNIX-Auditdateien hochladen, anhand derer ermittelt wird, ob ein getestetes System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.

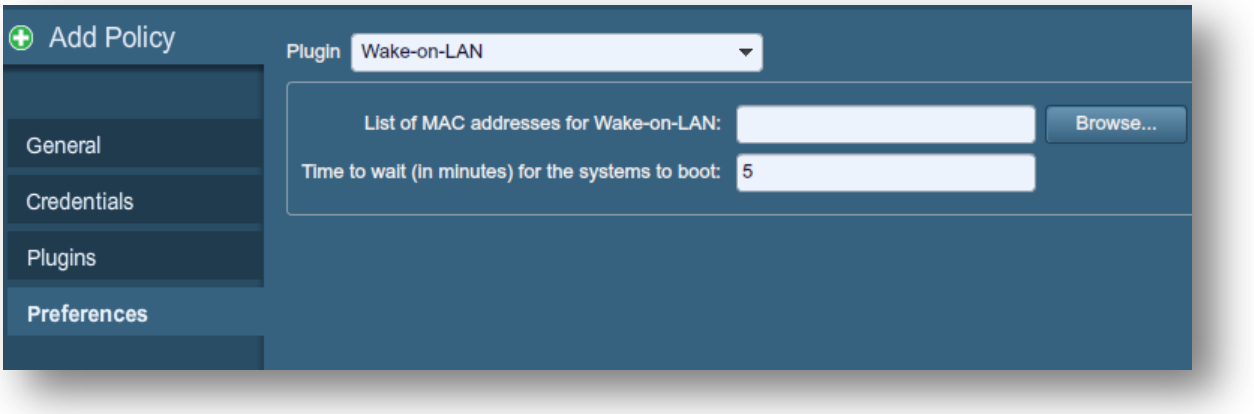
Über „**VMware SOAP API Settings**“ („VMware SOAP-API-Einstellungen“) können Nessus die Anmeldedaten übergeben werden, die erforderlich sind, um die Managementsysteme VMware ESX, ESXi und vSphere Hypervisor über die eigene SOAP-API zu authentifizieren (der SSH-Zugriff ist mittlerweile veraltet). Die API ist für Audits von vSphere 4.x-/5.x-, ESXi- und ESX-Hosts vorgesehen, jedoch nicht für auf den Hosts ausgeführte virtuelle Systeme. Mithilfe dieser Authentifizierungsmethode können authentifizierte Scans oder Complianceaudits durchgeführt werden.



Option	Beschreibung
VMware user name („VMware-Benutzername“)	Der für die Authentifizierung verwendete Benutzername. Bei integrierten Hosts oder lokalen Konten können die Anmeldedaten Active Directory-Konten sein, wobei sich das Konto in der lokalen Gruppe `root` befinden muss. Domänenanmeldedaten haben das Format „Benutzer@Domäne“, während bei lokalen Konten Benutzername und Kennwort angegeben werden müssen.
VMware password (unsafe!) (VMware-Kennwort – unsicher!)	Dieses Kennwort wird ungeschützt versendet und kann im Netzwerk von Dritten abgefangen werden.
Ignore SSL Certificate (SSL-Zertifikat ignorieren)	Wenn auf dem Server ein SSL-Zertifikat vorhanden ist, wird dieses ignoriert.

Über „**Wake-on-LAN**“ wird festgelegt, an welche Hosts vor der Ausführung eines Scans WOL-Pakete übermittelt werden sollen und wie lange auf den Start dieser Systeme gewartet werden soll. Die Liste der MAC-Adressen für die WOL-Funktion wird durch den Upload einer Textdatei festgelegt, in der jeweils eine MAC-Adresse pro Zeile aufgeführt ist. Beispiel:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[…]
```



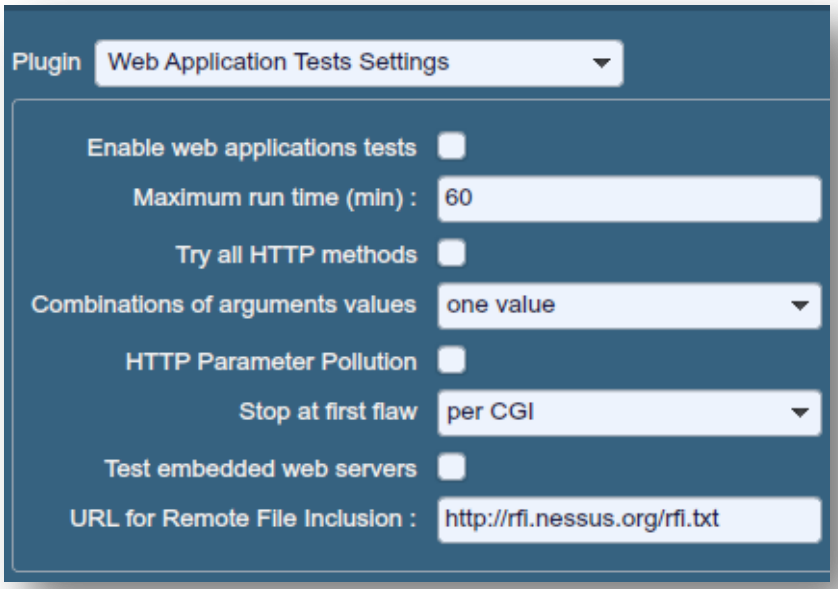
Über „**Web Application Tests Settings**“ („Einstellungen für Webanwendungstests“) werden die Argumente der Remote-CGIs (Common Gateway Interface) getestet, die beim Webspiegelungsprozess erkannt wurden. Hierzu wird versucht, verbreitete CGI-Programmierfehler wie Cross-Site Scripting, Remote File Inclusion, Befehlsausführung, Traversal-Angriffe oder SQL Injection zu übergeben. Sie aktivieren diese Option durch Markierung des Kontrollkästchens „Enable web applications tests“ („Webanwendungstests aktivieren“). Diese Tests erfordern die folgenden NASL-Plugins:

- 11139, 42424, 42479, 42426, 42427, 43160 – SQL Injection (CGI-Missbrauch)
- 39465, 44967 – Befehlsausführung (CGI-Missbrauch)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (CGI-Missbrauch: XSS)
- 39467, 46195, 46194 – Directory Traversal (CGI-Missbrauch)
- 39468 – HTTP Header Injection (CGI-Missbrauch: XSS)
- 39469, 42056, 42872 – File Inclusion (CGI-Missbrauch)
- 42055 - Formatstring (CGI-Missbrauch)
- 42423, 42054 - Server Side Includes (CGI-Missbrauch)
- 44136 - Cookiemanipulation (CGI-Missbrauch)
- 46196 - XML Injection (CGI-Missbrauch)
- 40406, 48926, 48927 - Fehlermeldungen
- 47830, 47832, 47834, 44134 - Weitere Angriffe (CGI-Missbrauch)

Hinweis: Diese Liste webanwendungsspezifischer Plugins wird regelmäßig aktualisiert. Sie kann unter Umständen unvollständig sein. Weitere Plugins können von den hier betroffenen Einstellungen abhängen.

Option	Beschreibung
Maximum run time (min) (Maximale Ausführungszeit (Min.)	Mithilfe dieser Option wird festgelegt, wie viel Zeit (in Minuten) für die Durchführung von Webanwendungstests aufgewendet werden darf. Die Vorgabe beträgt 60 Minuten und gilt für alle Ports und CGIs einer Website. Das Scannen des lokalen Netzwerks auf Websites mit kleineren Anwendungen wird in der Regel innerhalb einer Stunde abgeschlossen, doch kann für Websites mit umfangreichen Anwendungen ein höherer Wert erforderlich sein.
Try all HTTP methods (Alle HTTP-Methoden ausprobieren)	Standardmäßig testet Nessus nur unter Verwendung von GET-Anforderungen. Mithilfe dieser Option wird Nessus angewiesen, auch POST-Anforderungen zu verwenden, um die Überprüfung von Webformularen zu verbessern. Standardmäßig werden bei Webanwendungstests nur GET-Anforderungen verwendet, sofern diese Option nicht aktiviert ist. Im Allgemeinen verwenden komplexere Anwendungen die POST-Methode, wenn ein Benutzer Daten an die Anwendung übermittelt. Diese Einstellung ermöglicht umfassendere Tests, kann die erforderliche Zeit jedoch erheblich verlängern. Wird sie ausgewählt, dann testet Nessus jedes Skript und jede Variable sowohl mit GET- als auch mit POST-Anforderungen.
Combinations of arguments values (Kombinationen aus Argumentwerten)	Diese Option verwaltet die Kombination von Argumentwerten, die in HTTP-Anforderungen verwendet werden. Das Dropdownmenü enthält drei Optionen: „**One value**“ („Bestimmter Wert“): Hiermit wird immer nur ein Parameter gleichzeitig mit einem Angriffsstring getestet. „Angriffslose“ Varianten für weitere Parameter werden nicht ausprobiert. Beispielsweise würde Nessus „`/test.php?arg1=XSS&b=1&c=1`“ ausprobieren, wobei „b“ und „c“ andere Werte gestatten würden, ohne dass jede einzelne Kombination überprüft würde. Dies ist die schnellste Testmöglichkeit, bei der zudem die kleinste Ergebnismenge erzeugt wird. „**All pairs (slower but efficient)**“ („Alle Paare (langsamer, aber wirksamer)“): Dieser Testansatz ist etwas langsamer, aber wirksamer als der „One value“-Test. Beim Testen mehrerer Parameter werden ein Angriffsstring und Varianten für eine einzelne Variable getestet, und der erste Wert wird dann für alle anderen Variablen verwendet. Beispielsweise würde Nessus „`/test.php?a=XSS&b=1&c=1&d=1`“ ausprobieren und die Variablen dann nacheinander so abarbeiten, dass einer Variable der Angriffsstring übergeben wird, einer weiteren zyklisch alle möglichen Werte übergeben werden (wie sie beim Spiegelungsprozess ermittelt wurden) und alle anderen Variablen den ersten Wert erhalten. In diesem Fall würde Nessus niemals auf „`/test.php?a=XSS&b=3&c=3&d=3`“ prüfen, wenn der erste Wert jeder Variable „1“ wäre. „**All combinations (extremely slow)**“ („Alle Kombinationen (extrem langsam)“): Bei dieser Testmethode wird ein umfassender Test aller möglichen Kombinationen von Angriffsstrings mit gültigen Eingabewerten für die Variablen ausgeführt. Hierbei wird bei „All-pairs“ („Alle Paare“) zur Geschwindigkeitssteigerung versucht, eine kleinere Datenmenge zu erstellen, während bei „All combinations“ („Alle Kombinationen“) kein Kompromiss eingegangen wird – hier wird die gesamte Datenmenge für Tests verwendet. Beachten Sie, dass der Abschluss des Vorgangs bei dieser Testmethode **sehr lange** dauern kann.
HTTP Parameter Pollution	Beschreibt bei der Durchführung von Webanwendungstests den Versuch, vorhandene Filtermechanismen zu umgehen. Hierzu werden Inhalte in eine Variable injiziert, während gleichzeitig dieselbe Variable mit gültigem Inhalt übergeben wird. Ein normaler SQL-Injection-Test könnte etwa so aussehen: „`/target.cgi?a='&b=2`“. Mit aktivierter HTTP Parameter Pollution (HPP) sähe die Anforderung dann eher so aus: „`/target.cgi?a='&a=1&b=2`“.

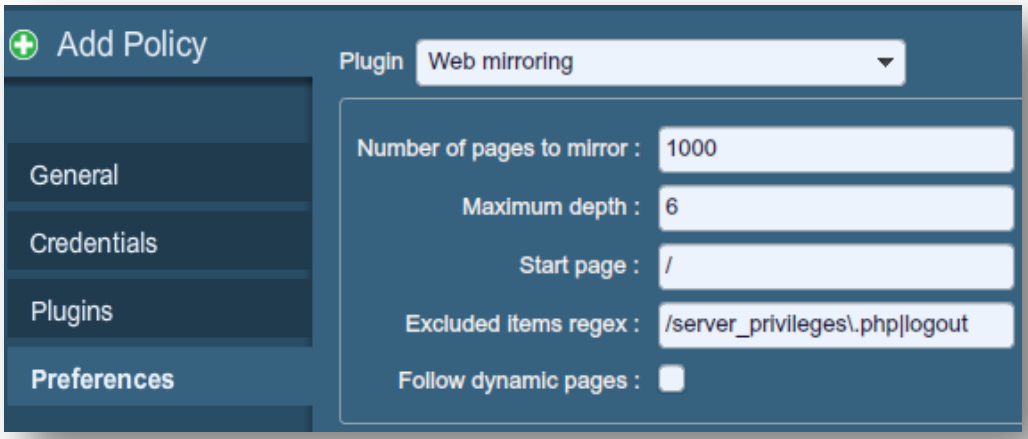
Stop at first flaw (Bei erstem Schwachpunkt anhalten)	Mit dieser Option wird bestimmt, wann ein neuer Schwachpunkt als Ziel verwendet wird. Dies betrifft die Skriptebene: Die Erkennung eines XSS-Schwachpunkts führt nicht zu einer Deaktivierung der Suche nach SQL-Injection- oder Header-Injection-Schwachpunkten; allerdings erhalten Sie maximal einen Bericht zu jedem Typ auf dem jeweiligen Port, sofern „Thorough tests“ („Umfassende Tests“) nicht festgelegt ist. Beachten Sie, dass mehrere Schwachpunkte desselben Typs (z. B. XSS, SQL usw.) gemeldet werden können, sofern sie vom selben Angriff erfasst wurden. Das Dropdownmenü enthält vier Optionen: „**Per CGI**“ („Je CGI“): Sobald ein Schwachpunkt von einem Skript in einem CGI gefunden wurde, wechselt Nessus zum nächsten bekannten CGI auf demselben Server bzw. – wenn kein CGI mehr vorhanden ist – zum nächsten Port oder Server. Dies ist die Grundeinstellung. „**Per port (quicker)**“ („Je Port (schneller)“): Sobald ein Schwachpunkt von einem Skript auf einem Webserver gefunden wurde, stoppt Nessus und wechselt zu einem anderen Webserver auf einem anderen Port. „**Per parameter (slow)**“ („Je Parameter (langsam)“): Sobald ein Schwachpunkttyp (z. B. XSS) in einem CGI gefunden wurde, wechselt Nessus zum nächsten Parameter desselben CGI, zum nächsten CGI oder zum nächsten Port oder Server. „**Look for all flaws (slower)**“ („Nach allen Schwachpunkten suchen (langsamer)“): Führt umfassende Tests unabhängig von den gefundenen Schwachpunkten durch. Diese Option kann einen sehr ausführlichen Bericht generieren. In den meisten Fällen ist von ihrer Verwendung abzuraten.
Test Embedded web servers (Eingebettete Webserver testen)	Eingebettete Webserver sind häufig statisch und enthalten keine anpassbaren CGI-Skripts. Zudem sind eingebettete Webserver möglicherweise absturzanfällig oder reagieren beim Scannen nicht mehr. Tenable empfiehlt das Scannen eingebetteter Webserver separat von anderen Webservern mithilfe dieser Option.
URL for Remote File Inclusion (URL für Remote File Inclusion)	Beim RFI-Test (Remote File Inclusion) gibt diese Option eine Datei auf einem Remotehost an, die für die Tests verwendet wird. Standardmäßig benutzt Nessus eine sichere Datei, die auf dem Webserver von Tenable gehostet und speziell für RFI-Tests vorgesehen ist. Kann der Scanner nicht auf das Internet zugreifen, dann wir die Verwendung einer intern gehosteten Datei für genauere RFI-Tests empfohlen.



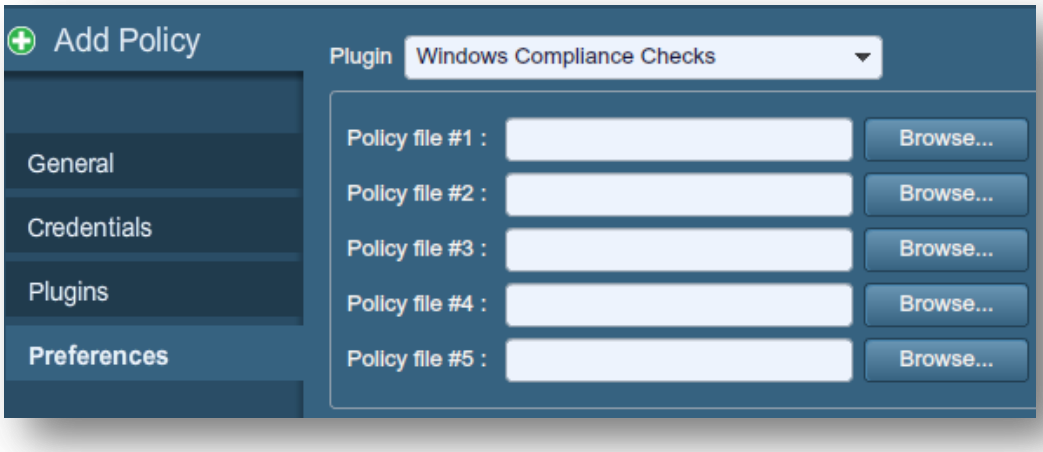
Mit „**Web Mirroring**“ („Webspiegelung“) werden Konfigurationsparameter für das native Nessus-Utility zur Spiegelung von Webserverinhalten festgelegt. Nessus spiegelt Webinhalte, um sie besser auf Sicherheitslücken prüfen zu können und die Auswirkungen auf den Server zu minimieren.

Wenn die Webspiegelungsparameter so festgelegt sind, dass eine gesamte Website gespiegelt wird, kann dies zu erheblichem Datenaufkommen während des Scans führen. Ist beispielsweise 1 GB Daten auf einem Webserver vorhanden und wurde Nessus so konfiguriert, dass alles gespiegelt wird, so wird beim Scan auch mindestens 1 GB Datenverkehr vom Server zum Nessus-Scanner generiert.

Option	Beschreibung
Number of pages to mirror (Anzahl zu spiegelnder Seiten)	Maximale Anzahl zu spiegelnder Seiten.
Maximum depth (Maximale Spiegelungstiefe)	Hiermit wird angegeben, wie vielen Links Nessus je Startseite folgt.
Start page (Startseite)	URL der ersten zu testenden Seite. Sind mehrere Seiten erforderlich, dann können diese durch einen Doppelpunkt getrennt angegeben werden (z. B. „/:/php4:/base“).
Excluded items regex (Regulärer Ausdruck für ausgeschlossene Elemente)	Hiermit wird der Ausschluss von Teilen der erfassten Website aktiviert. Um beispielsweise das Verzeichnis „/manual“ und alle Perl-CGIs auszuschließen, geben Sie folgenden Wert für dieses Feld an: `(^/manual)|(\.pl(\?.*)?$).`
Follow dynamic pages (Dynamischen Seiten folgen)	Wenn diese Option aktiviert ist, folgt Nessus dynamischen Links, wodurch die oben festgelegten Grenzwerte überschritten werden können.

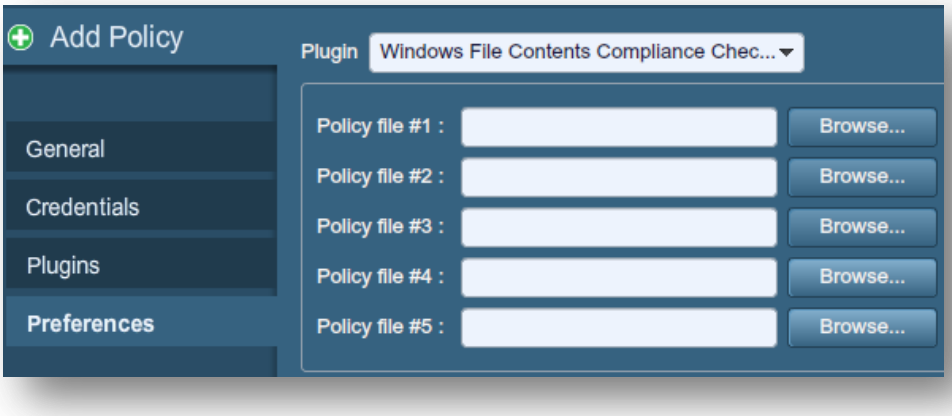


Mit der Option „**Windows Compliance Checks**“ („Windows-Compliancetests“) können ProfessionalFeed-Kunden Windows-Konfigurationsauditdateien hochladen, anhand derer ermittelt wird, ob ein getestetes System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



Mit der Option „**Windows File Contents Compliance Checks**“ können ProfessionalFeed-Kunden Windows-basierte Auditdateien hochladen, die nach bestimmten Inhaltstypen suchen (z. B. Kreditkarten, Social Security-Nummern usw.), und so die Compliance in Bezug auf Unternehmensrichtlinien oder Drittvorgaben bestimmen.

Wenn alle Optionen wie gewünscht konfiguriert wurden, klicken Sie auf „**Submit**“ („Absenden“), um die Richtlinie zu speichern und zur Registerkarte „Policies“ (Richtlinien) zurückzukehren. Sie können jederzeit auf „**Edit**“ („Bearbeiten“) klicken, um Änderungen einer Richtlinie vorzunehmen, die Sie bereits erstellt haben. Durch Anklicken von „**Delete**“ löschen Sie eine Richtlinie vollständig.



Weitere Informationen

Tenable hat eine Reihe von Dokumenten erstellt, in denen die Bereitstellung, die Installation, die Konfiguration, der Betrieb und die Testmethoden von Nessus ausführlich beschrieben werden. Es sind diese:

- **Nessus-Installationshandbuch** (Schrittanleitung zur Nessus-Installation)
- **Authentifizierte Nessus-Tests für UNIX und Windows** (enthält Informationen zur Durchführung authentifizierter Netzwerkscans mit dem Nessus-Sicherheitslückenscanner)
- **Nessus-Compliancetests** (allgemeiner Leitfaden zum Verstehen und Durchführen von Compliancetests mithilfe von Nessus und SecurityCenter)
- **Nessus-Referenzhandbuch für Compliancetests** (umfassender Leitfaden zur Syntax von Nessus-Compliancetests)
- **Nessus V2-Dateiformat** (beschreibt die Struktur des `.nessus`-Dateiformats, das mit Nessus 3.2 und NessusClient 3.2 eingeführt wurde)
- **Nessus XML-RPC-Protokollspezifikation** (beschreibt das XML-RPC-Protokoll und die Schnittstelle in Nessus)
- **Compliance-Überwachung in Echtzeit** (erläutert, wie die Lösungen von Tenable Sie bei der Erfüllung zahlreicher gesetzlicher Vorschriften und Finanzstandards unterstützt)
- **SecurityCenter-Administratorhandbuch**

Weitere Onlineressourcen sind nachfolgend aufgeführt:

- Nessus-Diskussionsforum: https://discussions.nessus.org/
- Blog von Tenable: http://blog.tenable.com/
- Podcast von Tenable: http://blog.tenablesecurity.com/podcast/
- Beispielvideos: http://www.youtube.com/user/tenablesecurity
- Twitterfeed von Tenable: http://twitter.com/tenablesecurity

Setzen Sie sich mit Tenable in Verbindung – via E-Mail (support@tenable.com, sales@tenable.com,) oder über unsere Website unter http://www.tenable.com/.

Wissenswertes zu Tenable Network Security

Tenable Network Security gehört zu den Marktführern im Bereich Unified Security Monitoring. Das Unternehmen entwickelt den Nessus-Sicherheitslückenscanner und bietet agentenlose Unternehmenslösungen für die fortlaufende Überwachung auf Sicherheitslücken, Konfigurationsfehler, Datenlecks, Protokollverwaltung und Risikoerkennung an, um die Sicherheit im Netzwerk und die Compliance in Bezug auf Standards wie FDCC, FISMA, SANS CSIS und PCI sicherzustellen. Die preisgekrönten Produkte von Tenable werden von zahlreichen Global 2000-Unternehmen und staatlichen Einrichtungen in aller Welt verwendet, um Risiken im Netzwerk proaktiv zu minimieren. Weitere Informationen finden Sie unter http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

Copyright © 2013. Tenable Network Security, Inc. Alle Rechte vorbehalten. Tenable Network Security und Nessus sind eingetragene Marken von Tenable Network Security, Inc.